Universidad Internacional de La Rioja
Máster Universitario en Estudios sobre Terrorismo (MET)

Deep web y monedas virtuales: entorno privilegiado para las organizaciones terroristas

Trabajo fin de Máster presentado por: Carlos Yuste González

Titulación: Trabajo fin de Máster

Director/a:Manuel Torres Soriano

CATEGORÍA TESAURO: 3.3.1

RESUMEN

Internet es una herramienta indispensable en la sociedad actual, estando presente en todas las facetas de nuestras vidas. Lo que ha supuesto, sin duda, un gran avance con innumerables ventajas tiene su reverso en el uso que del mismo da el terrorismo. La deep web, como parte de la red, supone un entorno privilegiado para sus fines ya que su propia estructura y filosofía está concebida para garantizar el anonimato de sus usuarios. Ante esa premisa, las organizaciones criminales y terroristas han hecho de ella un lugar de encuentro, donde poder comunicarse y actuar con seguridad y, al amparo de las condiciones de anonimato, han florecido mercados en los que es posible comprar, prácticamente, cualquier producto considerado ilegal. Para el éxito de estos mercados, y dada la trazabilidad de los medios de pago existentes por parte de las agencias y fuerzas policiales, surgieron las monedas virtuales, y más en concreto el Bitcoin, como piedra angular de los mismos, haciendo devenir en insuficientes las normativas nacionales sobre control de la financiación del terrorismo, de prevención del blanqueo y control de flujos entre países. La deep web y las monedas virtuales suponen, a la vez, una amenaza y un reto al que los países tienen que dar solución con urgencia.

PALABRAS CLAVE

DEEP WEB; DARK WEB; TOR; BLACK MARKETS; MONEDAS VIRTUALES; BITCOIN.

PREGUNTA INICIAL Y FORMULACION DE HIPOTESIS:

La deep web como herramienta favorecedora de las actividades terroristas

TESIS:

- Las monedas virtuales y, en especial, el Bitcoin juegan un papel importante en las actividades terroristas.

INDICE

1. – INTRODUCCIÓN

Desde su nacimiento, allá por la década de los ochenta, y la introducción del World Wide Web en el comienzo de los noventa, el crecimiento de la conocida como red de redes ha resultado ser exponencial. Lo que en principio estaba pensado por el científico británico Tim Berners-Lee para mejorar le gestión de información en el Centro Europeo de Física de Partículas (CERN), en Suiza, pronto se convirtió en, posiblemente, en una de las mayores revoluciones en la historia de la humanidad. Umberto Eco lo definió de forma magistral:

> El ordenador e Internet son la verdadera revolución del siglo y, como la imprenta, pueden modificar nuestra manera de pensar y de aprender. La prensa de Gutenberg produjo la libre interpretación de la Biblia, arruinó a los iluminados y provocó la aparición de una nueva pedagogía, basada en los libros y en las imágenes. Antes de la imprenta, un niño no podía acceder a un manuscrito. Hoy, con Internet, podemos saber cosas que nuestros antepasados tardaban una vida en conocer.

Con un crecimiento imparable y ayudado por la revolución en las conocidas como Tecnologías de la Información y la Comunicación, TIC´s, no ha dejado de ocupar nuevas parcelas de la vida de los seres humanos, llegando a extremos que hasta hace poco tiempo eran propios de una película de ciencia ficción.

La forma de comunicarse e interaccionar entre los seres humanos también se ha visto fuertemente afectada por esta revolución tecnológica. Internet se ha convertido, además, en punto de encuentro donde relacionarse, en detrimento de otras formas más tradicionales, o donde, incluso, se establecen nuevos lazos de relación con personas completamente desconocidas.

Tanto el terrorismo como la delincuencia organizada han sido capaces de evolucionar, como ya habían hecho anteriormente, y adaptarse a la tipología criminal que la red permite, siendo ésta, con los conocimientos técnicos necesarios, un lugar en el que se pueden mover con mayor facilidad que en el plano físico, aprovechándose de las posibilidades de permanecer anónimos dentro de la red y propiciando espacios de impunidad.

En el plano político, los distintos Estados se han ido percatando, de forma paulatina, de la amenaza que se cierne. Tarea compleja para los gobiernos de los países democráticos, ya que deben conjugar unas normativas sobre el uso de internet en las que éste siga un siendo un lugar libre y abierto, y conjugar, de forma simultánea, una legislación en la que se facilite la

persecución del delito que se comete utilizando la red como instrumento e impidiendo la existencia de "islas de impunidad" o, los conocidos en el plano internacional como "paraísos cibernéticos", en los que la actuación policial es poco menos que imposible.

El propio Secretario General de las Naciones Unidas, Ban Ki-moon, afirmó que "Internet es un excelente ejemplo de cómo los terroristas pueden actuar de manera verdaderamente transnacional. En respuesta a ello, los Estados deben pensar y funcionar de manera igualmente transnacional[1]".

La noción de jurisdicción nacional que mantienen nuestras normas procesales hace que los vehículos legales creados para conseguir el auxilio judicial internacional, tales como las comisiones rogatorias o los MLAT (Mutual Legal Assistance Treaty), no cumplan su objetivo, al ser excesivamente lentos y formalistas.

El objeto del presente trabajo pretende abordar el uso que hacen las organizaciones terroristas de lo que se conoce como deep web. Se pretende que partiendo de unas explicaciones básicas de conceptos técnicos que permitan a un lector no familiarizado con los términos empleados, comprender los distintos campos en los que están operando los terroristas en la red, la complejidad que una investigación por parte de las Fuerzas y Cuerpos de Seguridad de dicho fenómeno entraña y el empleo de las criptomonedas, con especial incidencia en la más empleada a día de hoy, el Bitcoin, como elemento facilitador para distintas transacciones comerciales, como puede ser la compra-venta de productos y servicios ilegales en los *black markets*, el lavado de dinero, etc. La complejidad del trabajo la confiere la escasa información fiable que se puede encontrar en fuentes abiertas en la actualidad y lo cambiante que es el campo objeto de estudio.

[1] UNDOC (Oficina de las Naciones Unidas contra la Droga y el Delito) "El uso de internet con fines terroristas" 2013. Disponible en: http://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/Use_of_Internet_Ebook_SPANISH_for_web.pdf

2.- ¿QUÉ ES LA DEEP WEB?

El término Deep Web fue acuñado por Michael K. Bergman[2], afirmando que realizar una búsqueda en Internet puede compararse a usar una red sobre la superficie del océano. Parte de la información será atrapada por la red, mientras la mayor parte se perderá porque la misma está profunda, no pudiendo ser recogida. Según este autor, en 2001, la información publicada en la Deep Web era de 7.500 terabytes, frente a los 19 terabytes de la conocida como Internet visible, es decir entre 400 a 500 veces mayor.

La Deep Web se refiere, pues, a aquella parte de la Web que no está indexada por los motores de búsqueda tradicionales como pueden ser Google, Bing o Yahoo, siendo, por tanto, muy difícil de rastrear, estando, además, muchos de los contenidos que allí anidan protegidos por mecanismos de seguridad tales como logins de identificación, contraseñas, etc.

Habitualmente, se suele utiliza la siguiente imagen para hacer una representación gráfica de lo que supone la Deep Web con respecto a la Web visible:

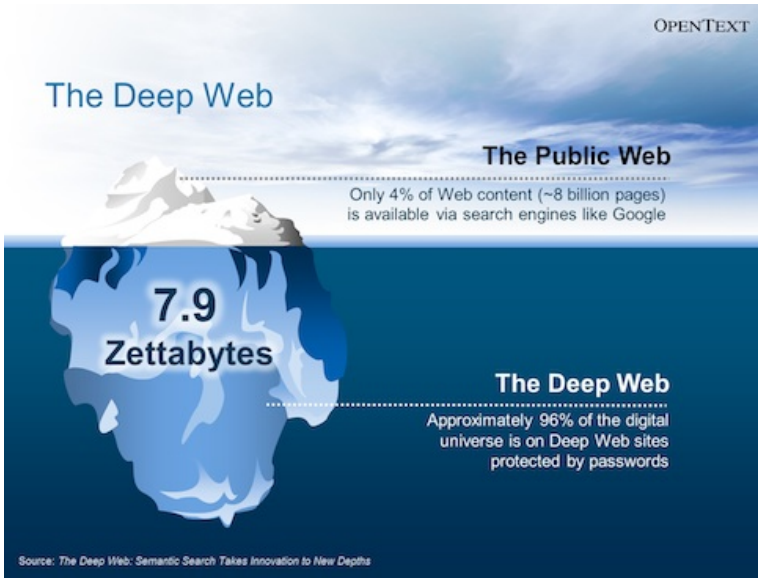

Figura 1[3]*Comparación de la Deep Web con la web pública. Fuente:* http://www.legaltechnology.com/wp-content/uploads/2013/07/The-Deep-Web.jpg

[2] Bergman, Michael K "The Deep Web: surfacing hidden value*" 2001. Disponible en* http://grids.ucs.indiana.edu/courses/xinformatics/searchindik/deepwebwhitepaper.pdf

[3] http://www.legaltechnology.com/wp-content/uploads/2013/07/The-Deep-Web.jpg

El término Dark Web, quizá, sea más adecuado para denominar aquellos sitios o páginas contenidos en las redes anónimas, de las que hablaremos posteriormente, siendo acuñado el término por cuatro investigadores de la empresa informática Microsoft[4] refriéndose a aquellas tecnologías de red que permitían distribuir contenido digital utilizando una red física subyacente, sobre la que implementar una aplicación o capa de protocolos de comunicación. El concepto evolucionó para añadir la necesidad de privacidad, tecnologías que permitían la transferencia de información sin que la identidad de los intervinientes o el contenido pudiese ser conocida.

Estos contenidos son accesibles a cualquier usuario mediante el empleo de proxies o de navegadores específicos diseñados para tal fin, proporcionando su uso anonimato, tanto al usuario que trata de acceder a la información, como al que lo publicó.

También habría que hacer mención a una clasificación que se ha desarrollado sobre distintos niveles de profundidad en base al tipo de contenidos y la gravedad o ilegalidad de los mismos[5], pudiendo tener su importancia desde el punto de vista policial o judicial, ya que a mayor profundidad los contenidos serán más graves.

Así tendríamos los siguientes niveles:

- Nivel 1. Surface Web. Correspondería con la Web superficial en la que navega la mayoría de la gente y en la que se sitúan sitios web como pueden ser Google, Facebook, etc.

- Nivel 2. Bergie Web. Correspondería con el resto de la conocida Web superficial, pero con unos contenidos que ya sí serían, en algunos casos, ilegales. Se encontrarían páginas con contenido porno, comunidad 4chan, o aquellas que violan derechos de propiedad intelectual como pueden ser servicios de televisión en streaming, o descarga o visión en streaming de películas o series.

- Nivel 3. Deep Web. En este nivel ya se requiere el empleo de un proxy de cara a preservar el anonimato. Entre los contenidos que se pueden encontrar en este nivel

[4] Biddle, P., England P., Peinado M. y Willman B., "The Darknet and the Future of Content Distribution". Microsoft Corporation. Disponible en: http://msl1.mit.edu/ESD10/docs/darknet5.pdf (enlace comprobado el 01-09-2015)

[5] En este sentido se pueden encontrar múltiples clasificaciones de carácter similar. Como ejemplo de las mismas: http://www.hablandodeciencia.com/articulos/2014/10/27/deep-web/ (enlace comprobado 01-09-2015)

destacaría la pornografía infantil, venta de sustancias estupefacientes o proselitismo del terrorismo islámico.

- Nivel 4. Charter Web. Se necesita el uso de Tor para navegar en este nivel. En este nivel se podrían encontrar los conocidos como foros underground, en los que se pueden adquirir sustancias estupefacientes, armas, así lo que constituiría el denominado "*crime as a service*", en el que se podrían contratar servicios criminales varios como el alquiler de una bootnet, una denegación de servicio, compras de tarjetas falsas, etc.

- Nivel 5. Marianas Web. Su contenido es muy restringido y, normalmente, de origen ilícito pero de extrema gravedad como pueden ser delitos de terrorismo, trata de seres humanos, etc.

3.- USO DE INTERNET POR PARTE DE LOS TERRORISTAS

Que los terroristas hacen uso de Internet es, a día de hoy, un hecho incuestionable que, además, se propaga con una rapidez inusitada. Las nuevas Tecnologías de la Información, TIC´s, han supuesto un nuevo ámbito de relación, que no es otro que el ciberespacio. Éste ha conseguido eliminar barreras y fronteras en la comunicación entre las personas a nivel mundial, siendo posible la transmisión de información de forma inmediata y, en la medida en que interese a los actores intervinientes, de forma completamente anónima.

Las conocidas como TIC´s son, hoy en día, una herramienta fundamental en el desarrollo económico y social de un país, siendo prácticamente imposible concebir el mundo tal cual lo conocemos hoy en día sin su concurrencia.

Los movimientos terroristas, a la par que la criminalidad organizada, vieron en Internet un medio para conseguir ciertos objetivos que resultaban, en muchos casos, más fáciles de obtener que en el mundo físico, ya que aprovechaban las ventajas que les proporcionaba este nuevo modo de trasmisión de la comunicación y la información. Este medio multiplicaba la efectividad en la elaboración de sus planes de acciones armadas y, además, pronto se vio que era un medio privilegiado para el reclutamiento y captación de nuevos adeptos a la causa

terrorista. Gabriel Weimann[6] afirmaba ya en el año 2004 que Internet era un medio ideal para las actividades terroristas, enumerando una serie de ventajas que ofrecería este medio para ese tipo de organizaciones, como serían:

- Un acceso sencillo.
- Ausencia de regulación o, en caso de existir, muy limitada.
- Difícil censura por parte de las autoridades; unas audiencias potenciales que se extenderían al mundo entero.
- Anonimato en las comunicaciones.
- Un flujo de la información muy rápido.
- Mínimo coste económico por el mantenimiento de una presencia en la web.
- Un entorno multimedia.
- Capacidad de dar forma a la cobertura en los medios de comunicación tradicionales, que usan, cada vez con mayor frecuencia, Internet como fuente de información para dar a conocer historias.

Abu Musab Zarqawi pronto fue consciente del potencial que tenía Internet para difundir y publicitar sus acciones. Susan B. Glasser y Steve Coll[7] afirmaron que "nunca una organización terrorista había tenido tanto éxito entrelazando su guerra real, sobre el terreno, con su yihad electrónica, haciendo los especialistas en la materia del grupo de Zarqawi lo que los expertos afirman será el futuro de la guerrilla insurgente, donde no habrá acto que no sea grabado y las atrocidades parecen ser cometidas para ser filmadas y distribuidas de forma instantánea en Internet". Éste declaró en Global Islamic Media Front, medio que distribuía muy a menudo mensajes de él por internet, que "la tecnología de internet lo facilita todo".

[6] Weimann, G. "Terror on the Internet: The New Arena, The New Challenges" United States Institue of Peace. 2004. Disponible en: http://www.usip.org/events/terror-the-internet-the-new-arena-the-new-challenges (enlace comprobado el 01-09-2015)

[7] Glasser, S. y Coll, S. "The Web as Weapon" The Washington Post. 2005. Disponible en: http://www.washingtonpost.com/wp-dyn/content/article/2005/08/08/AR2005080801018.html (enlace comprobado el 01-09-2015)

Además afirmaba que las páginas de la web son "la forma para que todo el mundo en el mundo entero escuchasen a los mujaheddin".

G. Weimann[8] afirmó que "el terrorismo postmoderno es menos centralizado, menos estructurado, menos organizado, y bastante más peligroso que el terrorismo de finales del siglo XX". Internet ha expandido su teatro de operaciones, permitiéndoles tener un control absoluto sobre sus comunicaciones a través del uso de la infraestructura del ciberespacio desarrollada por el mundo civilizado".

Bin Laden realizó un uso muy intenso de las tecnologías de la información cuando se encontraba en su cuartel general en Afganistán, gracias a un sistema que le habían instalado miembros egipcios de su propia organización terrorista[9].

Jordán también cita el uso de la red por otros grupos terroristas, como puede ser el caso de Hamas, grupo que de forma habitual la emplea para coordinar actividades, lo cual dificulta la labor de los servicios de inteligencia israelís debido al ingente volumen de tráfico de información y, añade, al uso de programas de encriptación.

El empleo de Internet como elemento propagandístico es, sin lugar a dudas, el primer ejemplo de uso intensivo por parte de organizaciones de la red. El profesor Torres[10] definió tres etapas en la acción propagandística del GJM:

1. Primera fase. Métodos tradicionales, personalismo y nebulosa informativa (1994- 11 de septiembre de 2001)

2. Segunda fase: Las recompensas del terror (11-S-primavera de 2003).

3. Tercera fase: Dispersión de la producción propagandística y primacía de internet (primavera 2003-….). En esta fase es cuando se produce la expansión en el uso de la red con fines propagandísticos, con una producción descentralizada e inmensa, que ha logrado la concesión de una especie de saturación propagandística que ha hecho que

[8] Weimann, G. Obra citada

[9] Jordán, J. "El terrorismo en la sociedad de la información. El caso de Al Qaida". El profesional de la información, volumen 11, número 4, julio-agosto 2002. Página 300 (citando a Arquilla, Ronfeldt, Zanini, 1999 "Networks, netwar and information age terrorism". Rand, Santa Monica.

[10] Torres, M.R., "El eco del terror. Ideología y propaganda en el terrorismo yihadista". Madrid: Plaza y Valdés. (2009). Páginas 149 y siguientes.

los medios de comunicación presten menos atención a sus videos, optando los terroristas difundan la práctica totalidad de sus documentos en internet. Ello se ha visto facilitado por las nuevas generaciones de jóvenes seguidores: con un internet con alcance casi universal y a un coste relativamente bajo, los jóvenes influenciados por la ideología yihadistas tienen ahora un origen urbano, con acceso a la red y muy apegados al uso de las conocidas como redes sociales.

Redes sociales comunes, de empleo universal como Facebook, Twitter o Instagram son empleados intensamente por los nuevos terroristas o por simpatizantes. Este uso que es, en principio, una amenaza por el alcance que puede tener la divulgación de la información, es, a la vez, una oportunidad para los servicios de inteligencia y de lucha antiterrorista de los distintos países.

Kalev Leetaru, experto en inteligencia sobre el Medio Este de la Universidad de Georgetown, afirma que el ISIL es el primer grupo que usa "los medios de comunicación social como un arma de guerra"[11]. Para él estos medios de comunicación social son una espada de doble filo, ya que los analistas de inteligencia pueden descubrir cosas que los combatientes no desean revelar.

Como hemos podido ver, Internet se ha convertido en un pieza habitual e indispensable en la actuación diaria de las organizaciones terroristas en general, y de las de corte yihadista en particular. Comenzaron haciendo un uso intenso de la misma con fines propagandísticos, ampliando a otras facetas, como pueden ser el reclutamiento de nuevos seguidores al movimiento yihadista e incluso, en algunos casos, la movilización de los mismos para luchar en los conflictos en marcha; planificación y coordinación de acciones, etc.

3.1.- ESTRATEGIA DE SEGURIDAD NACIONAL

La repercusión y proyección de futuro como amenaza del terrorismo empleando Internet como medio para verificarlo queda patente en hechos como que en España, en el capítulo 3 de la Estrategia de Seguridad Nacional de 2013 recoge como un riesgo y amenaza para

[11] Kalev Leetaru. Citado por Daileda, C. y Franceschi-Bicchierai, L. "U.S. Intelligence Officials want ISIL fighters to keep Tweering". Marshable. 2014. Disponible en: http://mashable.com/2014/07/11/us-wants-iraq-radicals-to-tweet/ (Enlace comprobado el 01-09-2015)

la seguridad nacional las ciberamenazas, afirmando que "la dependencia de la sociedad del ciberespacio y su fácil accesibilidad hacen que cada vez sean más comunes y preocupantes las intromisiones en este ámbito. En buena medida, el ciberespacio es un medio para la materialización de otros riesgos y amenazas. Los ciberataques, ya sean en sus modalidades de ciberterrorismo, ciberdelito/cibercrimen, ciberespionaje o hacktivismo, se han convertido en un potente instrumento de agresión contra particulares e instituciones públicas y privadas". A continuación destaca que "el bajo coste y mínimo riesgo que suponen para el atacante y su fácil empleo, efectividad y accesibilidad, son factores que explican la extensión del fenómeno".

Igualmente la Estrategia de Ciberseguridad Nacional, impulsada en el año 2013 por el Consejo de Seguridad Nacional, procura dar respuesta a lo que considera el enorme desafío que supone la preservación del ciberespacio de los riesgos y amenazas que se ciernen sobre él[12]. Así, su Línea de acción 4 versa sobre la "Capacidad de investigación y persecución del ciberterrorismo y la ciberdelincuencia", dibujando un escenario en el que habrá de potenciarse las capacidades de los organismos públicos competentes para erradicar las posibles actividades delictivas y terroristas en el ciberespacio. El combate que habrá de librarse contra el terrorismo y el crimen organizado que actúan en el ciberespacio se concentra en su doble vertiente de instrumento facilitador y objeto directo de su acción.

4.- ACCESO A LA DEEP WEB Y A LA DARK WEB

El hecho de que Internet sea un medio en el que tanto organizaciones criminales como terroristas operen con una frecuencia inusitada con respecto a los niveles existentes hace tan sólo una década se debe, principalmente, a las posibilidades de anonimato y, por tanto, de impunidad que este medio las proporciona. Hay que reseñar que no todo el que emplea algún medio de anonimización es, per se, alguien que está en disposición de cometer un ilícito penal, sino que, en ocasiones, se trata de usuarios de la red que tratan de preservar, a toda costa, que se conozca su identidad, o bien puede ser empleado para saltar los filtros de acceso de los ISPs nacionales en países que tratan de someter a censura a la red.

[12] Estrategia de Ciberseguridad Nacional. Presidencia del Gobierno de España. 2013. Disponible en: http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf (enlace comprobado el 01-09-2015)

La navegación anónima es uno de los aspectos que causan mayor dificultad a las fuerzas y cuerpos de seguridad a la hora de investigar posibles delitos cometidos por los ciberterroristas o los ciberdelincuentes. El uso de dos o varios de los procedimientos existentes de forma entrelazada garantiza, prácticamente, su total anonimato. Más tarde detallaremos alguno de estos procedimientos, centrándonos ahora en la puerta de acceso tanto a la Deep Web como a la Dark Wek, que se realizará a través de serie de redes descentralizadas con una serie de nodos anónimos entre las que estarían incluidas la red I2P (Invisible Internet Proyect) y el modo empleado mayoritariamente en la actualidad: la red Tor.

4.1.- TOR

La red conocida como Tor debe su nombre a las siglas en inglés "The Onion Router", o también conocido como encaminador cebolla. Su origen se debe al trabajo realizado en el año 2003 por Roger Dingledine, Nick Mathewson y Paul Syverson a partir del proyecto desarrollado por el Laboratorio Naval de los Estados Unidos conocido como Onion Router en el año 2004. Desde 2005 hasta la actualidad pertenece a la fundación sin ánimo de lucro Tor Project[13].

Tor es un software libre multiplataforma que implementa una red de comunicaciones distribuida, cifrada, de baja latencia y superpuesta a internet. En ella el enrutamiento de paquetes se realiza ocultando la dirección IP de los usuarios logrando así el anonimato en la capa IP o de red.

Para que esto sea posible es imprescindible que el camino o ruta sea impredecible y, en la medida de lo posible, oculto, de forma que cada nodo sólo conozca el nodo anterior, del cual recibe el mensaje y el nodo siguiente, al cual enviará el mismo, sin que pueda saber si tanto el uno como el otro son o no los nodos iniciales o finales respectivamente. Este nodo final, si la comunicación es realizada con una entidad fuera de la red "onion", enviará su mensaje o petición en abierto, es decir, no irá cifrado. La red Tor crea, por defecto, rutas de tres nodos, siendo posible configurar este número e, incluso, utilizar tan sólo un nodo como router de entrada y salida, lo que no es muy aconsejable cuando de preservar el

[13] Para conocer más acerca del proyecto TOR se puede consultar el enlace: https://www.torproject.org/ (Enlace comprobado el 01-09-2015)

anonimato se trata. Los circuitos tienen una vida de diez minutos para seleccionar, posteriormente, una nueva ruta[14].

El esquema de funcionamiento, de forma abreviada, sería la siguiente:

- Si Alice quiere enviar un mensaje a Bob por medio de la red Tor, antes, su ordenador realizará una conexión a un servidor que contendrá las direcciones de los nodos de esta red.

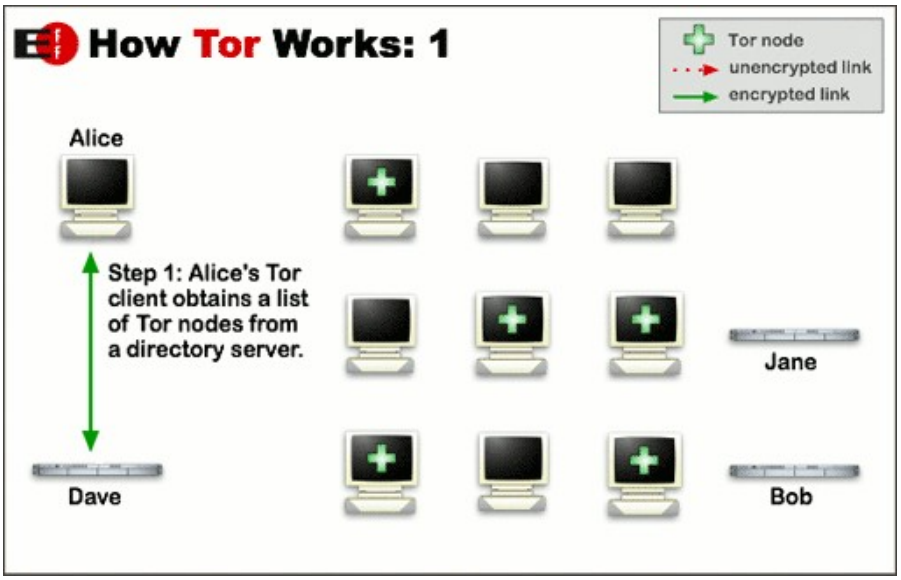

Figura 2. Fuente: https://www.torproject.org

- Tras recibir la lista de direcciones de este servidor, el cliente Tor instalado en el ordenador de Alice se conectará a un nodo aleatorio por medio de una conexión encriptada. Este nodo se conectará con otro nodo aleatorio de forma cifrada hasta llegar al denominado nodo de salida, donde la información dejará de estar cifrada y llegará a Bob en claro.

[14] Fisher, D. "¿Qué es TOR?". Blog Kaspersky. 2013.Disponible en: https://blog.kaspersky.es/que-es-tor/716/ (enlace comprobado el 01-09-2015)

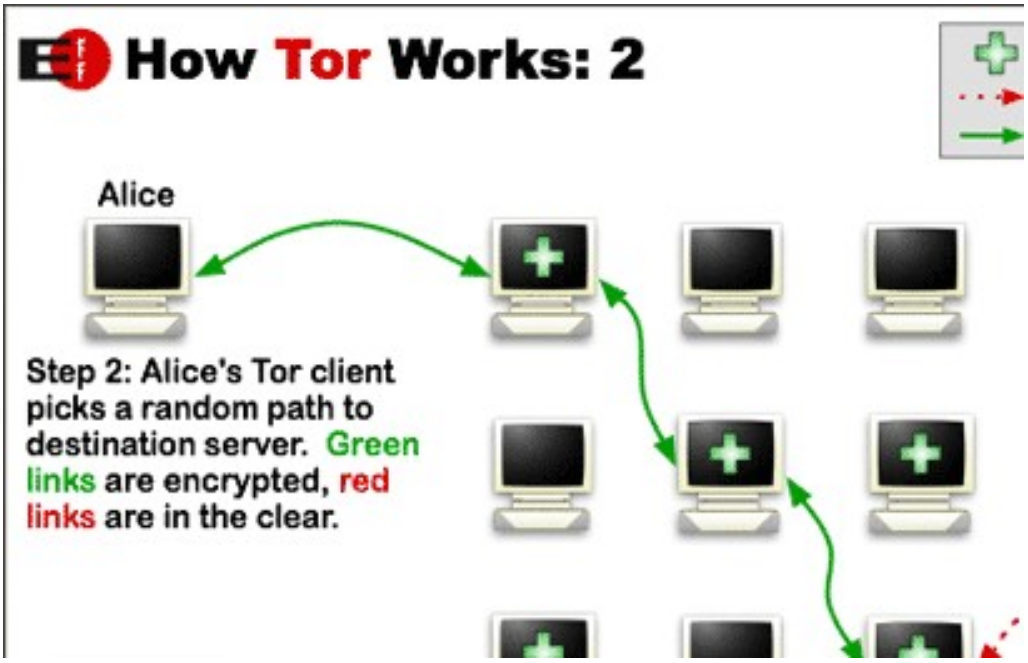

Figura 3. Fuente: https://www.torproject.org

- Si ahora Alice quiere comunicar o enviar un mensaje a Jane, el proceso será el mismo, pero el cliente Tor instalado en el ordenador de Alice escogerá otra ruta aleatoria y distinta a la anterior.

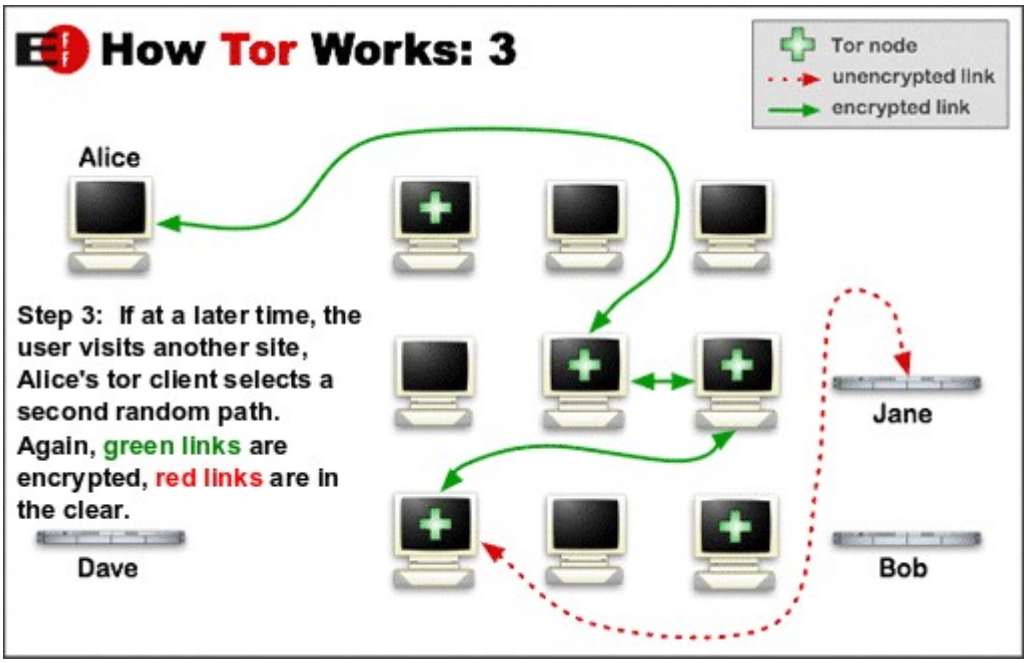

Figura 4. Fuente: https://www.torproject.org

La red Tor no está exenta de críticas debidas, fundamentalmente, a dos aspectos: las sospechas surgidas a raíz de las revelaciones de Snowden en las que alguna agencia de inteligencia de los EEUU podría haber estado recopilando información sobre la actividades en la red Tor, aprovechando algún bug del navegador Firefox; y a su baja velocidad, que podría ser corregido si popularizara la red HORNET, que alcanzaría velocidades de proceso de tráfico de hasta 93 GB/s[15].

4.1.1- HIDDEN SERVICES

Los Hidden Services o servicios ocultos[16] son la principal característica de Tor y la gran ventaja que tiene sobre otros medios de comunicación anónima, ya que permiten desarrollar y ofrecer un servicio sobre internet (como pueden ser una página Web, un chat, un servidor de correo, etc.) sin que ninguno de sus usuarios sepa realmente cual es su ubicación. Así, tanto usuario como proveedor de servicios establecen una conexión a través de la red Tor sin que éstos se conozcan.

La explicación del procedimiento, a grandes rasgos podría ser la que sigue[17]:

1. Se da de alta un servicio, generándose un descriptor que contendrá la clave pública del servicio y los nodos desde donde hay un circuito de conexión o punto de introducción. Contiene una secuencia de 16 caracteres seguidos de un sufijo .onion, anunciándose en bases de datos distribuidas que almacenan tablas de descriptores.

[15] Curthbertson, A. "HORNET: TOR-style dark web networks allows high-speed anonymus web browsing" International Business Times. 2015. Disponible en: http://www.ibtimes.co.uk/hornet-tor-style-dark-web-network-allows-high-speed-anonymous-web-browsing-1512359 (enlace comprobado el 01-09-2015)

[16] Para conocer más acerca de los Hidden Services del Proyecto TOR se puede consultar https://www.torproject.org/docs/tor-hidden-service.html.en (Enlace comprobado el 01-09-2015)

[17] Instituto Nacional de Cibeeerseguridad. "Anonimato e Internet.¿Ilusión o realidad? Navegando en la deep web". 2013. Disponible en: https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/anonimato_internet_deep_web (enlace comprobado el 01-09-2015)

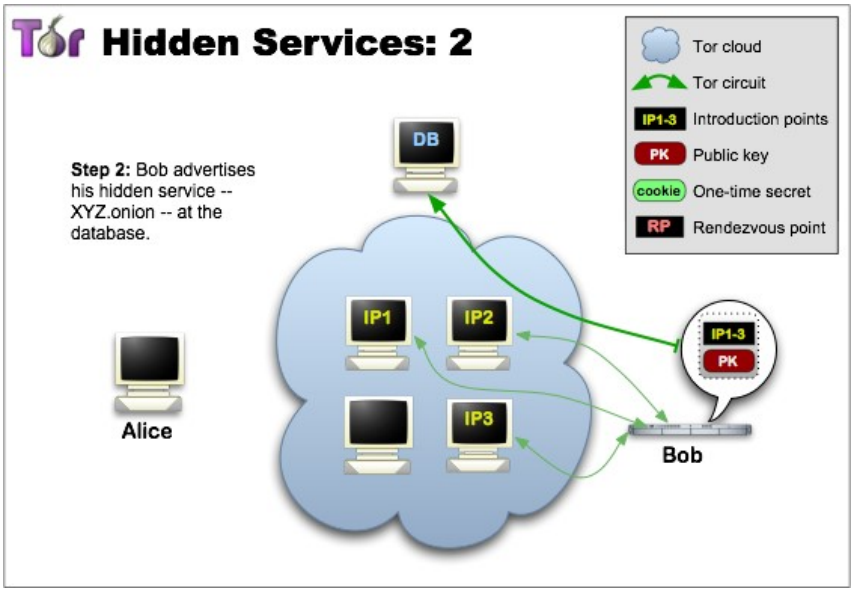

Figura 5. Fuente: https://www.torproject.org/docs/hidden-services.html.en

2. El cliente solicita al descriptor de la base de datos conocer la clave pública del servicio y el punto de introducción con el que comunicar para acordar una conexión. Se envía un mensaje al punto de introducción proponiendo al servicio en tercer nodo que actúe de ralay o punto de encuentro entre ambos. A la vez se envía una cookie que actuara de clave temporal en la comunicación.

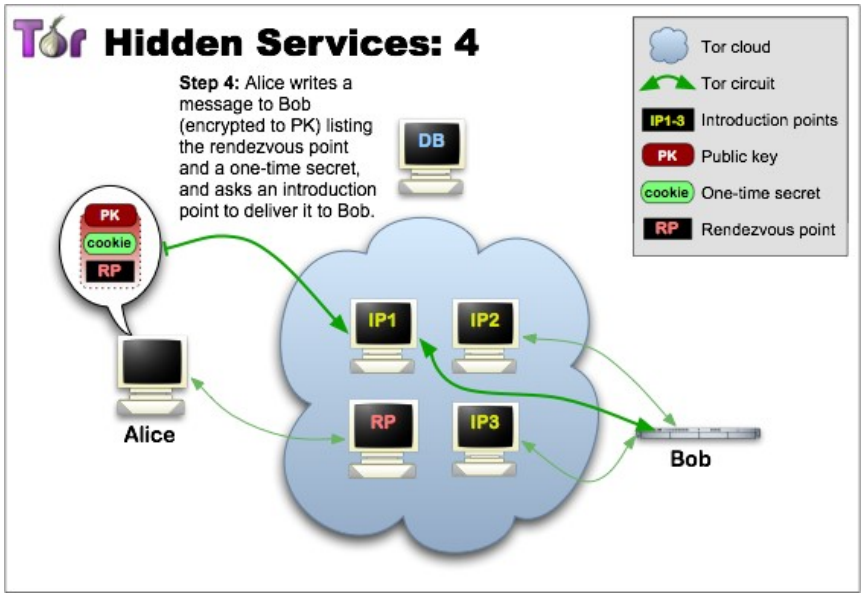

Figura 6. Fuente: https://www.torproject.org/docs/hidden-services.html.en

3. De este modo debido a que la conexión entre ambos a este punto de encuentro intermedio es mediante Tor, la comunicación entre cliente y servicio es totalmente anónima.

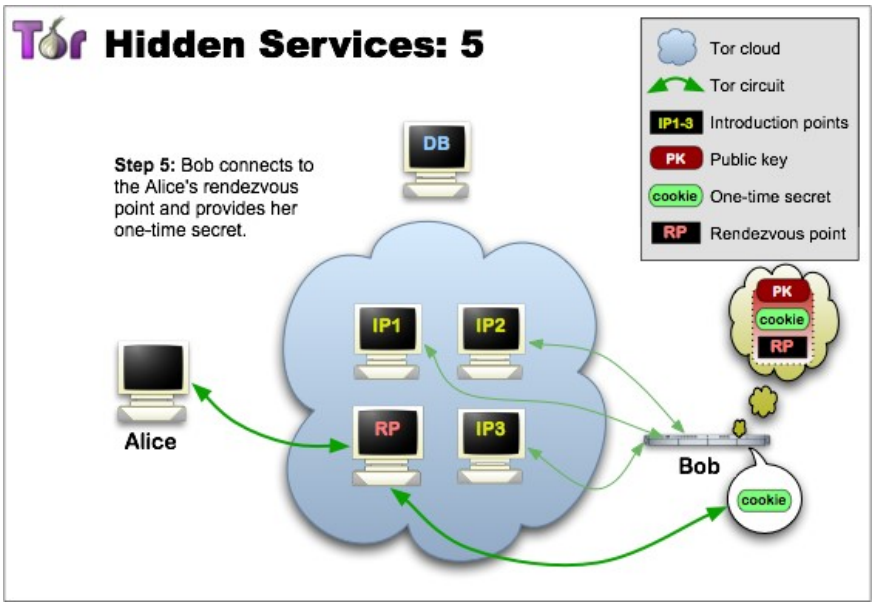

Figura 7. Fuente: https://www.torproject.org/docs/hidden-services.html.en

4.2.- I2P

The Invisible Internet Project[18] es una red anónima, superpuesta, distribuida y cifrada extremo a extremo con cuatro capas de cifrado empleadas cuando se envía un mensaje. Es una red descentralizada o entre iguales (P2P), siendo obligatorio formar parte de la Red y enrutar comunicaciones para acceder a la misma. Por cada tipo de servicio se crea un túnel de entrada y otro de salida por el que envía sus mensajes, no estando los usuarios identificados por su IP, por lo que se consigue el anonimato. Esta es, por tanto, la primera diferencia reseñable con respecto a Tor, el que los circuitos son unidireccionales y no bidireccionales, por lo que para comunicar dos usuarios será necesaria la creación de cuatro túneles, uno de entrada y uno de salida por cada uno.

[18] Para conocer más acerca del Proyecto del Internet Invisible se puede consultar el enlace https://geti2p.net/es/ (enlace comprobado el 01-09-2015)

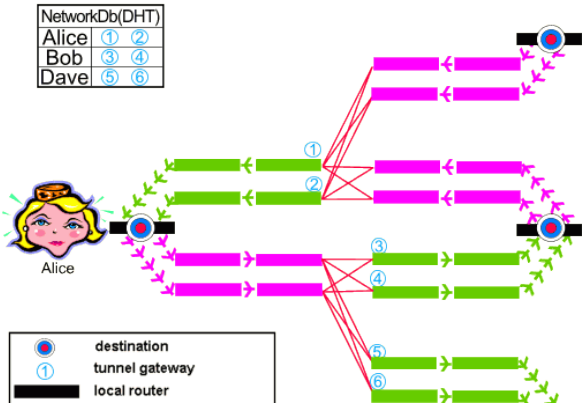

Figura 8. Fuente: https://geti2p.net/es/docs/how/intro

En la actualidad el número de usuarios de I2P es mucho menor que el de Tor, debido, en parte, a que el modelo distribuido que emplea obliga a todo usuario a participar en la red como router, lo cual es una ventaja, ya que evita sobrecargas por el excesivo número de usuarios respecto al de nodos router, siendo menos vulnerable a ataques de denegación de servicio. Además, su menor tamaño ha supuesto una ventaja hasta el momento en cuanto a su seguridad, ya que no ha focalizado la atención del movimiento hacktivista o de gobiernos interesados en mantener una censura en la red o la violación del anonimato que proporciona.

5.- USO DE LA DARK WEB POR LOS TERRORISTAS

El empleo de la deep web, y más en concreto, la dark web, por parte de organizaciones terroristas es un hecho, aumentando cada día el empleo de la misma debido a las condiciones de seguridad que le confiere y, además, el elevado volumen de recursos que pueden encontrar en la misma y que faciliten y potencien sus actividades.

Es compleja la elaboración, a priori, de una correlación de usos que dichas organizaciones estén haciendo de este medio, debido, en parte, a la propia idiosincrasia del medio al que nos referimos y, por otro lado, a que la información existente al respecto tan sólo se puede encontrar en fuentes cerradas con nivel alto de clasificación, lo cual, indudablemente, excede en mucho las posibilidades de este trabajo.

No obstante, vamos a intentar hacer una relación de usos que pueden estar haciendo de la Internet profunda, empleando como guía el documento publicado por Naciones Unidas en

2013, elaborado, en concreto, por la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) en colaboración con el Equipo Especial sobre la Ejecución de la Lucha contra el Terrorismo, titulado "El uso de internet con fines terroristas"[19]. En dicha obra han optado por adoptar un enfoque funcional en relación con la clasificación de los medios por los cuales se suele utilizar Internet para promover los actos terroristas y prestarles apoyo.

5.1.- PROPAGANDA, RECLUTAMIENTO, INCITACIÓN Y RADICALIZACIÓN

El empleo de Internet para la promoción de la ideología extrema y la violencia que la acompaña ha tenido como resultado el incremento exponencial, a nivel mundial, de las personas que pueden ser receptoras de dicho mensaje. Otra característica es la posibilidad que los propios grupos terroristas tienen de distribuir directamente su contenido a través de Internet, por lo que su dependencia de los medios o canales tradicionales de comunicación ha disminuido drásticamente, llegando, incluso, a invertirse en alguna ocasión, incluso, el proceso normal de la comunicación siendo los medios de comunicación quienes se habrían interesado por reproducir videos subidos por los terroristas.

Éstos han optado por el empleo de plataformas de redes sociales con una implantación masiva como Twitter y Facebook, como medio para distribuir su mensaje y conseguir captar nuevos seguidores y, tras un seguimiento de posibles nuevos adeptos, optan por contactar con ellos por medios de mensajería instantánea como what´s app para, posteriormente y si se comprueba que la evolución ideológica y posibilidades de radicalización son positivas, llegar al contacto directo. Por otro lado han procurado el empleo de sitios web muy populares como puede ser Youtube para poder subir sus videos propagandísticos, además del empleo de empresas que ofrecen servicios web de alojamiento de archivos de gran tamaño, como puede ser RapidShare o Mega.

En un principio, los grupos terroristas crearon sus propios sitios web de carácter oficial, pero tras el 11-S sufrieron un incesante hostigamiento por parte, tanto de servicios de inteligencia como de la comunidad hacker, lo cual les obligo a un constante peregrinar por la red en busca

[19] Obra citada. Disponible en: www.unodc.org/documents/terrorism/Publications (enlace comprobado el 01-09-2015)

de alojamientos y dominios que propició su paulatina desaparición[20]. En esos momentos, además, era muy difícil mantener un dominio debido a que la contratación de debía hacer con cargo a una tarjeta de crédito lo cual delataría la identidad del pagador. Posteriormente optaron por el pago de tarjetas robadas, pero una vez el fraude era descubierto el servicio quedaba cancelado. En la actualidad esos problemas los pueden solventar los terroristas con facilidad acudiendo a las posibilidades que la dark web les brinda: emplean una identidad falsa adquirida en un *dark market*, y buscarían empresas que presten ese servicio y admitan el pago en bitcoins, como digitalvalley, namecheap, allwebs.host, etc., que como veremos más adelante, garantizaría en total anonimato de quien realiza el pago.

Respecto al cierre, por parte de las autoridades, de los distintos foros o salas de chat de inclinación yihadista que se podían encontrar en la conocida como surface web, ya en el año 2007 Mark Burguess, director del Instituto Mundial de Seguridad de Bruselas advertía que "demasiado énfasis en el cierre de sitios web también podría ser contraproducente, ya que es probable que las fuerzas del sitio web terroristas terminen pasando a la clandestinidad, a la llamada Deep Web o internet oculto"[21]

Como bien define la UNODC, el reclutamiento, la radicalización y la incitación al terrorismo pueden considerarse como puntos a lo largo de un continuo. En el mismo, y para fortalecer esos lazos, pueden jugar un papel fundamental el uso de salas chat o de foros.

Respecto a dichas salas chat o foros se pueden encontrar en la deep web multitud de los mismos, beneficiándose de las condiciones de anonimato que proporciona la red TOR, con una estructura similar, en cuanto a jerarquía, a la de los foros tradicionales que se pueden encontrar en la surface web: administradores, situados en la cúspide de la estructura y con acceso a todas las funcionalidades; moderadores, con la función de vigilar las normas y condiciones de uso; por último nos encontraríamos con los usuarios comunes.

En algún foro el acceso se haría, exclusivamente, por invitación de algún individuo que ya estuviese integrado en el mismo y con cierta reputación, poniendo ésta como garantía y aval para que el nuevo miembro fuese admitido, siendo un buen método para limitar la posible infiltración.

---

[20] TORRES SORIANO, M. "Terrorismo yihadista y nuevos usos de Internet: la distribución de propaganda". Real Instituto Elcano. ARI número 110/2009

[21] www.deepweb.es/la-yihad-y-el-terrorismo-en-la-deep-web/

Además, en caso de querer mandar mensajes privados a miembros del foro guardando mayores medidas de seguridad, se recurriría a la encriptación. Para ello podrían emplear soluciones comerciales o de software libre como PGP o GPG4USB, o podrían recurrir a programas propios de encriptación, evitando así la sospecha, en muchas ocasiones psicosis, de una posible puerta trasera de las aplicaciones comerciales que pudiesen ser utilizadas por las agencias de inteligencia. Un ejemplo sería el programa de encriptación conocido como Asrar al-Mujahideen, muy popular tras ser anunciado en la revista Inspire. En 2013 lanzaron Asrar al-Dardashah, un plug-in para mensajería instantánea. En junio de 2014, el Comité Técnico Al-Fajr (FTC), lanzó una versión para dispositivos móviles con sistema operativo Android de su programa de encriptación Amn Al-Mujahid, accesible en el sitio web www.alfajrtaqni.net, así como sus manuales de uso.

Figura 9. Fuente: www.alfajrtaqni.net

Con el empleo de la encriptación en los mensajes, bien enviados por medio del foro, bien enviados por mail, se logra que las comunicaciones sean aún más seguras dado que aunque el foro estuviese infiltrado por alguna agencia de inteligencia o lo estuviese siendo el servicio de

mail empleado por los terroristas, el uso de la encriptación hace casi imposible la posibilidad de llegar a poderse leer el mensaje en claro sin la contraseña. Los sistemas de cifrado basados en el algoritmo AES (Advance Encryption Standard), que se emplea en la actualidad como estándar de cifrado por todo el mundo y que la propia NSA americana recoge como estándar de encriptación con el que los documentos clasificados del Gobierno Americano, hacen prácticamente inviable, con el desarrollo tecnológico existente a día de hoy, la posibilidad de romper la cifra por medio de un ataque por fuerza bruta o mediante un ataque por reducción del número de rondas utilizado para la codificación. Por tanto, los terroristas que estén basando sus comunicaciones en un foro en la red Tor y, además empleen un sistema de cifrado como puede ser AES, pueden tener la tranquilidad de que es prácticamente imposible que una agencia de inteligencia consiga leer en claro el contenido de su mensaje.

5.2.- FINANCIACIÓN

Internet se ha revelado como un canal muy importante para la obtención de fondos económicos con los que financiar a grupos y células, o, directamente, actos de terrorismo. La UNODC afirma que los terroristas pueden recurrir a la recaudación de fondos y recursos en Internet de acuerdo a cuatro categorías: recaudación directa; comercio electrónico; empleo de los servicios de pago en línea y contribuciones a organizaciones benéficas.

Ciñéndonos al objeto de este trabajo, el uso de la deep web por parte de las organizaciones terroristas, podemos destacar las posibilidades que la misma tiene para que grupos terroristas puedan obtener financiación comenzando por la petición de fondos para sufragar sus actividades. La recaudación directa se realizaría utilizando sitios web y foros, comunicaciones directas a los posibles simpatizantes en las que se les solicitaría una donación, etc. En un principio, los sitios web o foros admitían que la transferencia de los fondos se realizase por medio de transferencias electrónicas. Sin embargo, en la actualidad, optan por solicitar los donativos por un medio que asegure el anonimato de ambas partes, teniendo el protagonismo en este punto el Bitcoin.

A continuación podemos ver la pantalla principal de un sitio web alojado en Tor en el que solicitan donaciones para la yihad en Bitcoin, facilitando el identificador de su monedero virtual.

Figura 10. Fuente: http://teir4baj5mpvkg5n.onion

5.2.1. - BLACK MARKETS

Cualquier organización, sea cual fuere su objetivo o ideología, tiene, necesariamente, la necesidad de recabar fondos con los poder mantener su estructura y poder llevar a cabo sus fines u objetivos. Las organizaciones terroristas no son una excepción ya que necesitan una gran cantidad de fondos para poder mantener sus planes, entrenamiento de sus operativos, mantenimiento de la infraestructura incluyendo pisos de seguridad, actividades de propaganda y, por supuesto, sufragar el coste del vivir día a día de sus miembros operativos[22].

[22] ASHLEY, Sean P., "The future of Terrorist Financing: Fighting terrorist financing in the digital Age", Penn State Journal of International Affairs. (2012). Página 9-26

La descentralización y fragmentación de muchas organizaciones terroristas, particularmente de Al Qaeda, trajo consigo que las células locales debían proveerse, por si mismas, de los medios económicos para mantener su actividad terrorista. Un método común que han empleado, de forma habitual, es el tráfico de sustancias estupefacientes a pequeña escala, dada la facilidad y rapidez con que dicha actividad que les reportaba fondos. Pero la misma llevaba aparejados muchos riesgos, como es una eventual intervención policial que, además de poder acarrear la detención del individuo, por añadidura, podría perjudicar seriamente a la organización al poner el foco de atención de los servicios de información de la policía sobre la célula terrorista dando al traste con sus actividades.

Un método muy empleado tanto por criminales como por terroristas para la obtención de fondos con las que sufragar sus actividades, empleando Internet, ha consistido en acudir a los *black markets* que hay en la dark web, y, muy especialmente, en especial en Tor. En estos mercados de lo ilegal se puede adquirir, hoy en día, prácticamente cualquier cosa que sea considerada ilegal, como puede ser la adquisición de sustancias estupefacientes, armas de fuego, documentos de identidad, servicios de hacking, servicio de sicarios, y un largo etcétera que ha modificado, de forma sustancial, el mapa criminal a nivel mundial, al tener cualquier persona con unos mínimos conocimientos en informática acceso a servicios criminales que harían el trabajo por él, contratando los servicios en la red y pagando en bitcoins. Es lo que se conoce como "*crime as a service*".

A modo de ejemplo y para ilustrar gráficamente lo expuesto más arriba, se adjuntan imágenes de qué tipo de productos se pueden adquirir en estos *black markets*, obtenidas de varios de ellos a mediados del mes de agosto de 2015:

Figura 11. Sitio en dark web venta armas

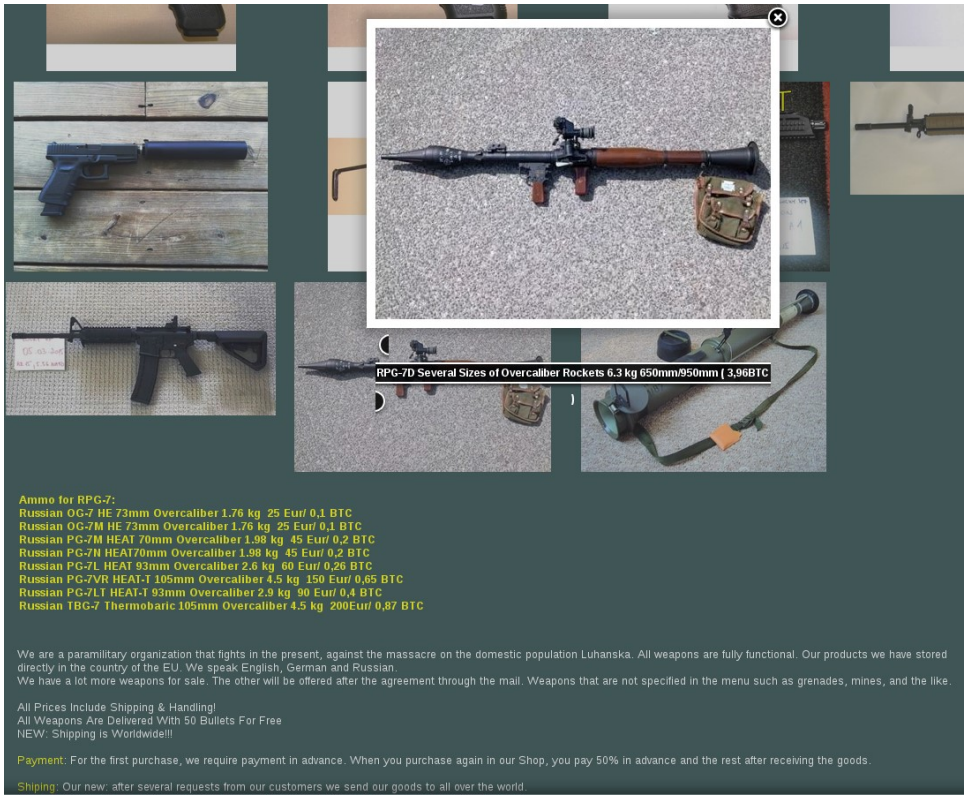

Figura 12. Oferta de lanzagranadas

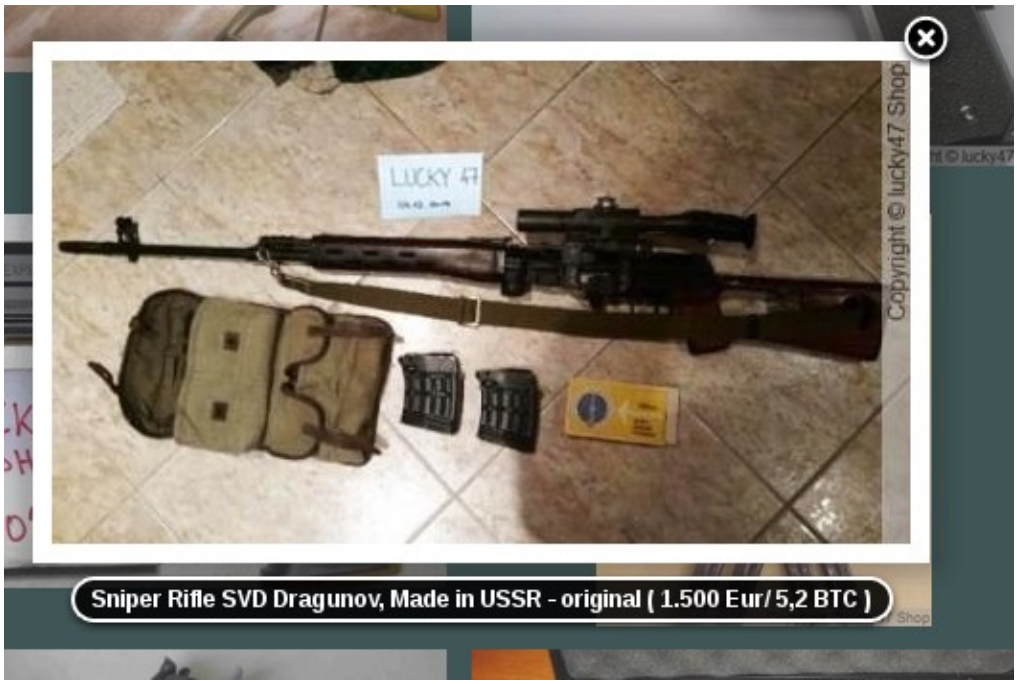

Figura 13. Oferta rifle de francotirador

REAL FRENCH PASSPORT+BIO METRIC DATAS

THANKS TO OUR METHOD ALREADY TESTED WE ARE ABLE TO BYPASS ALL THE SECURITIES OF THE ADMINISTRATION AND OBTAIN AFTER LESS 1 MONTH OF WORK A REAL FRENCH PASSPORT. IT ALLOWS YOU TO TRAVEL ALMOST EVERYWHERE AND PASS EASILY THE FRONTIERS BECAUSE IT S A REAL AND OFFICIAL DOCUMENT. IT S A CLONE ID. YOU ARE EVEN ABLE TO GO IN USA AND TAKE ADVANTAGE ON US CUSTOM WE JUST NEED THE FULLZ OF A SAME AGE...

Sold by castortroy75002 - *0* sold since *Jul 3, 2015* **Level 1**

	Features		Features
Product class	Physical package	**Origin country**	France
Quantity left	1 items	**Ships to**	Worldwide
Ends in	Never	**Payment**	Escrow

Default - 1 days - USD +0.00 / item

Purchase price: USD 1,645.84

Qty: 1 Buy Now Queue

6.1825 BTC

Description | Bids | Feedback | Refund Policy

Product Description

THANKS TO OUR METHOD ALREADY TESTED WE ARE ABLE TO BYPASS ALL THE SECURITIES OF THE ADMINISTRATION AND OBTAIN AFTER LESS 1 MONTH OF WORK A REAL FRENCH PASSPORT.

IT ALLOWS YOU TO TRAVEL ALMOST EVERYWHERE AND PASS EASILY THE FRONTIERS BECAUSE IT S A REAL AND OFFICIAL DOCUMENT.
IT S A CLONE ID.
YOU ARE EVEN ABLE TO GO IN USA AND TAKE ADVANTAGE ON US CUSTOM

WE JUST NEED THE FULLZ OF A SAME AGE PERSON AND SAME RACE SAME SEX.
FOR THE REST IS QUITE EASY.

THE ONLY THING STRESSFUL WILL BE THE DAY YOU NEED TO PUT YOUR FINGERPRINTS IN A MACHINE TO CAPTURE THEM AND YOUR FACE FOR THE OFFICIAL PICTURE DURING YOUR APPOINTMENT TO THE MAYOR.
WE WILL ARRANGE SOMETHING IN THE END OF FRIDAY AFTERNOON WHEN THE LAZY FROGGIES ADMINISTRATIVE AGENTS ARE JUST THINKING ABOUT THEIR DEPARTURE FOR THE WEEK END
ANYWAY IF YOU WANT A REAL DOCUMENT WE CAN T DO IT INSTEAD OF YOU.

THE SECOND TIME YOU WILL NEED TO PICK IT UP IN THE SAME PLACE AFTER TWO WEEKS JUST AFTER YOUR FIRST APPOINTMENT ,BUT THIS TIME YOU CAN COME WHENEVER, THE PASSPORT WILL BE AVAILABLE IN THE STORAGE OF AN ADMINISTRATIVE AGENT IT S QUITE EASY

IT S BETTER IF YOU ARE ABLE TO UNDERSTAND THE FRENCH IF NOT WE CAN PREPAIR AN INVALID CARD AND WE PRETEND YOU ARE A MENTAL DEFICIENT LOL WE CAN PAY SOMEONE TO BRING YOU BUT BEING FRENCH SPEAKING IS BETTER OR IF YOU DON T IT S TIME TO TAKE LESSONS. SO NO PANIC YOU ARE NOT OBLIGED TO SPEAK JUST FOLLOW THE INSTRUCTIONS OF THE AGENT.

THIS KIND OF PRODUCT IS IDEAL FOR PEOPLE UNDER ARREST OR WANTED.

Figura 14. Oferta documento identidad francés falso

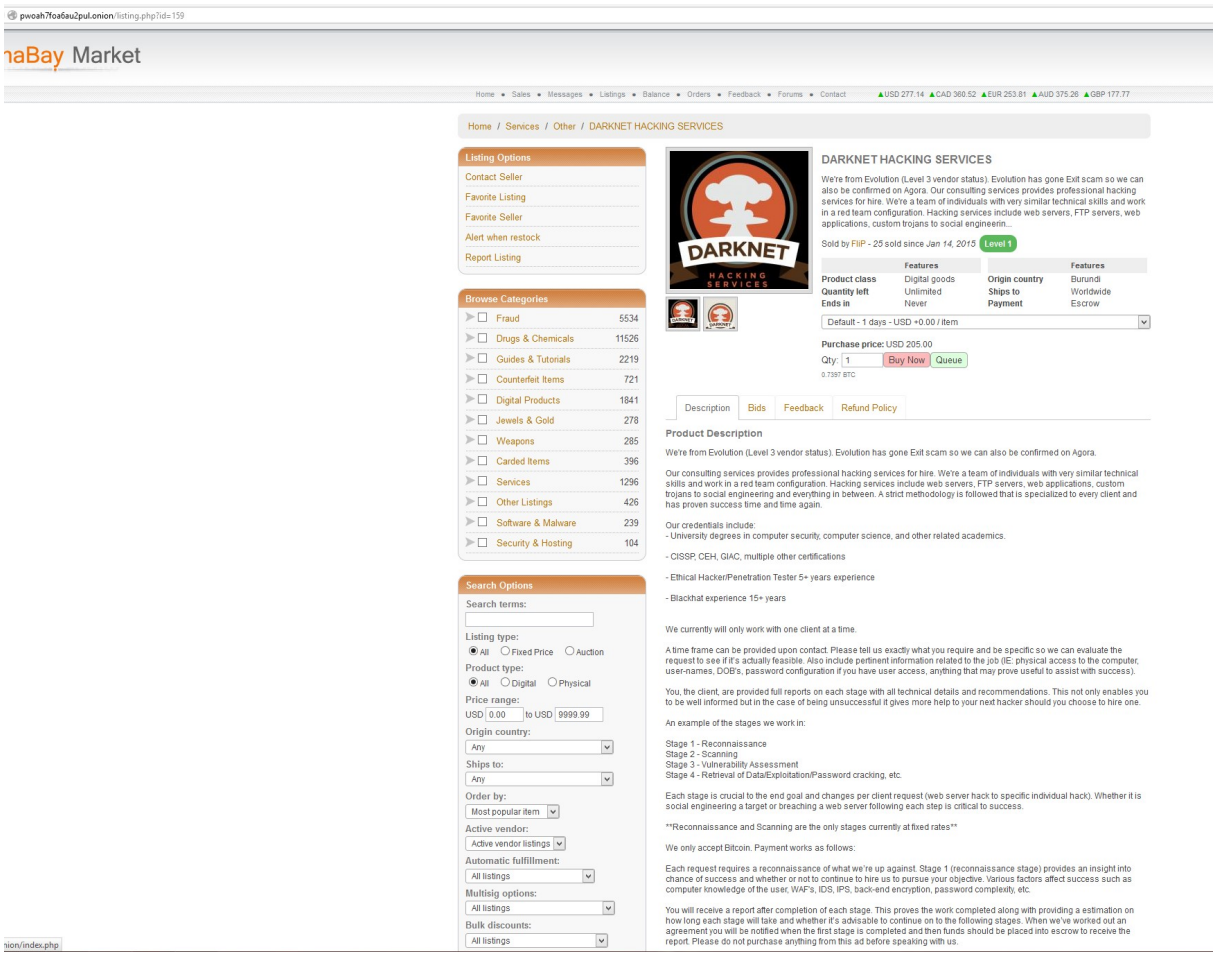

Figura 15. Oferta servicios de hacking

Para la financiación de esas células locales un método muy empleado es adquirir tarjetas de crédito robadas adquiridas en los referidos *black markets*.

Ya en 2005, las autoridades británicas detuvieron a un muchacho de 22 años, llamado Younis Tsouli, conocido en la dark web por el nickname Irhabi007 (Terrorista007). Este joven, autoradicalizado y autodidacta en el uso de internet, además de asesorar a operativos y adeptos en la fabricación de bombas e impartir seminarios on-line de cómo navegar por Internet de forma que no fuese posible su detección, resultó ser muy activo en la adquisición en los *black markets* de las numeraciones de tarjetas de crédito sustraídas, con las que obtenía fondos que blanqueaba, entre otros métodos, por medio de sitios web de juego y apuestas. Las autoridades británicas calcularon que Tsouli había conseguido en cargos a dicho tipo de tarjetas de crédito hasta el momento de su detención de 3.5 millones de dólares[23] de las

[23] JACOBSON, M., "Terrorist Financing on the Internet". CTC Sentinel. June 2009. VoL 2. Issue 6. Página 18

37.000 numeraciones de tarjetas sustraídas que fueron encontradas en su ordenador, intervenido en el momento de su detención por los investigadores británicos.

En estos *black markets* es realmente fácil encontrar vendedores de la numeración de tarjetas de crédito. Funcionan como sitios web muy conocidos en el que los vendedores tienen un ranking de puntuación que evalúa su reputación respecto a la fiabilidad del bien o servicio que vende. A continuación vemos algún ejemplo:

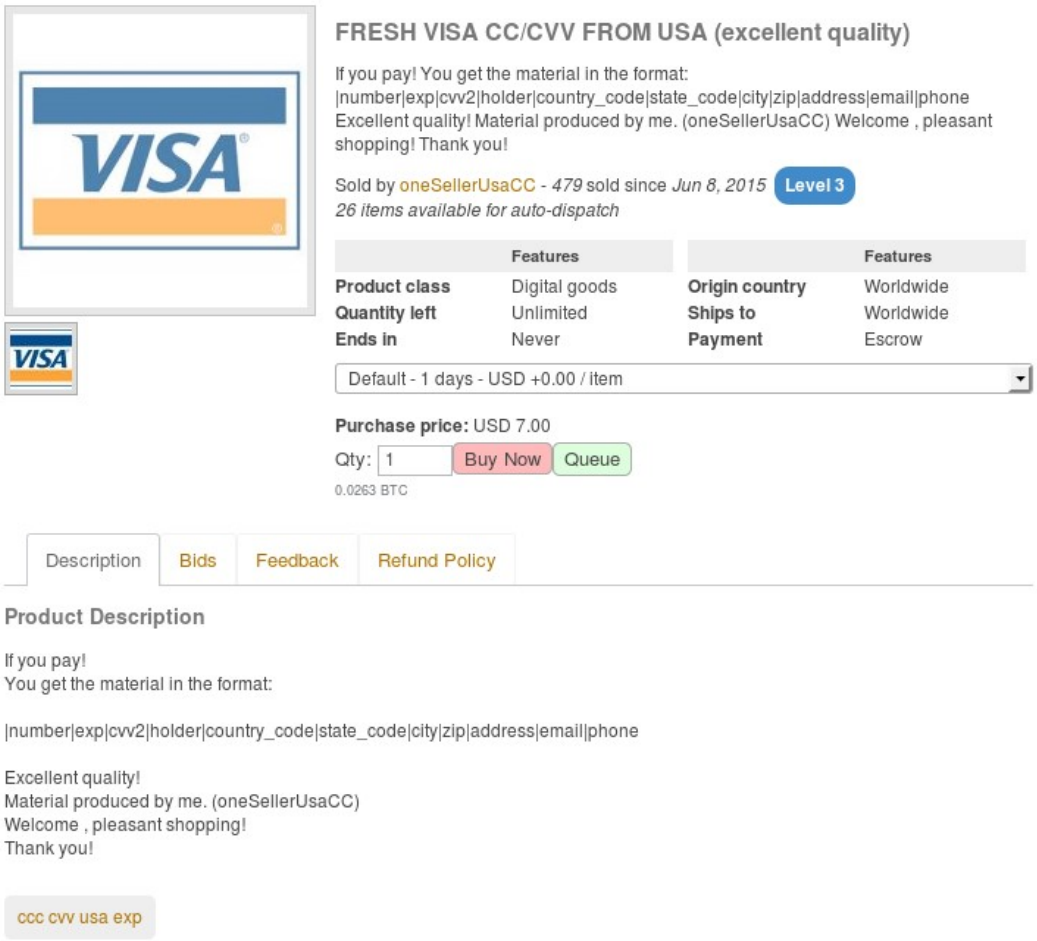

Figura 16. Venta numeración tarjeta crédito

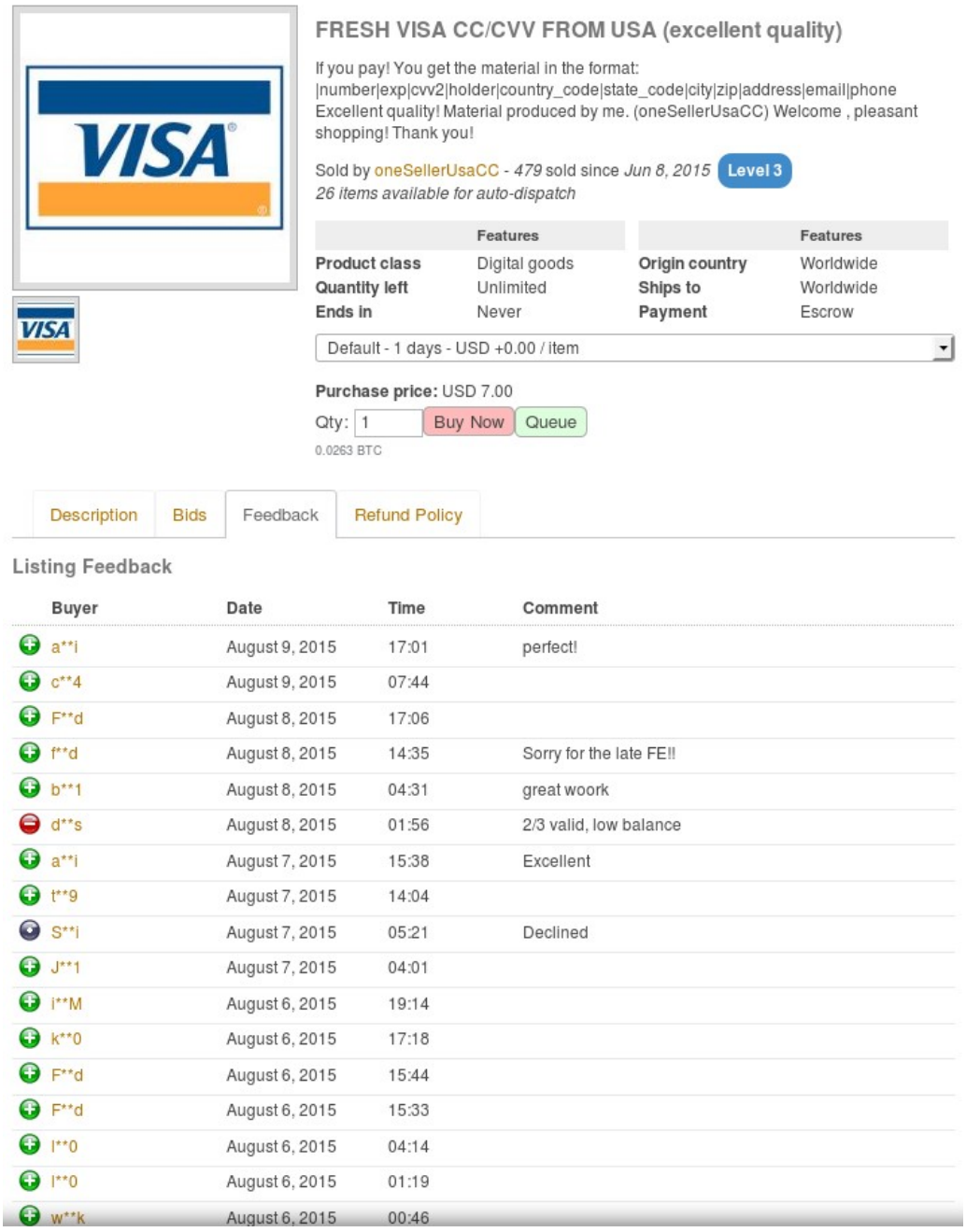

Figura 17. Feedback de compradores

En origen, para el pago, se admitía satisfacer la deuda mediante tarjetas de prepago, como Ukash o PaySafecard, cuyo funcionamiento es muy similar ya que se pueden adquirir en determinados comerciales, no requieren identificación para su compra y pueden ser utilizadas en las tiendas que operan en internet que aceptan este medio de pago, siendo la ventaja más acusada de su uso el anonimato que proporcionan en sus transacciones on-line. En la actualidad la práctica totalidad de ellos han abandonado ese tipo de pago para pasar al que, sin

lugar a dudas, es el más seguro, por el anonimato que confiere, para los criminales y terroristas que venden y compran en esos lugares de la red, el Bitcoin.

Algunos *black markets* dan un paso más en lo que a condiciones de anonimato y ocultación de cualquier rastro que pudiese dar una pista al investigador. Nos estamos refiriendo a los conocidos como mixers. En este tipo de "marketplace" comprador y vendedor no se relacionan directamente a la hora de efectuar el pago, funcionando de forma similar a la de conocidas pasarelas de pago como puede ser PayPal. El comprador a quien realmente da los bitcoins de la compra es al administrador de marketplace quien los retiene en espera de que el comprador no presente alguna queja acerca de su adquisición. Una vez las partes están conformes el administrador no pagará al vendedor directamente sino que para ocultar la transacción de forma que sea imposible relacionar comprador y vendedor, moverá los bitcoins a través de otras muchas cuentas, creando transacciones ficticias y mezclando éstas con las transacciones de otros usuarios. Mediante este procedimiento es imposible para el investigador poder relacionar mediante el marketplace al comprador con vendedor, no ya como prueba para un eventual procedimiento penal, sino tampoco a nivel de elaboración de inteligencia, lo que les convierte en un entorno privilegiado para las actividades de los criminales y los terroristas.

5.3.- CIBERATAQUES: ESPECIAL REFERENCIA A ATAQUES A INFRAESTRUCTURAS CRÍTICAS

Con respecto a los ciberataques, podríamos englobar todo aquel acto que desarrollan los terroristas, amparándose en las posibilidades que les proporciona la deep web, contra otros sitios webs o sistemas informáticos, siendo de especial importancia por la gravedad de las consecuencias, los que se efectúan a las infraestructuras críticas. Dado lo extenso de este apartado y que nos desviaría de su objetivo original, vamos a hacer una breve referencia a los mismos.

El Secretario de Defensa de los Estados Unidos, Leon Panetta, declaró en Octubre de 2012 que su país se enfrentaba a la posibilidad de un "ciber Pearl Harbor". "Un agresor, nación o grupo extremista, podía usar esa clase de ciber-herramientas para conseguir el control de

infraestructuras críticas[24]" Se refirió, como ejemplo, el ataque que sufrió en agosto de ese año la empresa saudí de petróleo, Aramco, que fue infectada por un malware que dejo inservibles 30000 ordenadores. En una línea argumental similar se pronuncia E. Kaspersky: "me temo que si nos enfrentamos con el terrorismo, será impredecible, en un lugar impredecible, pero con unos daños muy visibles. Desafortunadamente, habrá, posiblemente, muchas víctimas[25]". En el mismo artículo de prensa, Hilbert, ex agente en cibercrimen y ciberterrorismo del FBI, declaró que "hay cientos de ataques teniendo lugar contra la industria nuclear y el sistema financiero del Reino Unido y los Estados Unidos todos los días"

El ministro de Asuntos Exteriores, señor García Margallo, en declaraciones realizadas en febrero de este año fue en 2014, afirmaba que España, con más de 70000 ciberincidentes, era el tercer país en el mundo por incidencia, tan sólo superado por EEUU y Reino Unido[26].

Lo cierto es que en este tipo de ataques no queda clara la autoría, pudiendo provenir de otros países, como fue el ataque a la compañía cinematográfica Sony, donde todo indica que fue orquestado por Corea del Norte, o el hackeo a 19000 webs francesas por parte de yihadistas desde la red Tor consistentes en un defacement[27], como respuesta a la amenaza de venganza de Anonymus contra sitios webs de aquellos por el atentado a Charlie Hebdo

[24] Buniller, E. y Shanker, T., Panetta warns of dire threat of cyberattack on U.S.". The New York Times. 2012. Disponible en: http://mobile.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?_r=1&referrer= (enlace comprobado el 01-09-2015)

[25] Ellyatt, H. "Cyberterrorits to target critical infrastructure". CNBC. 2015. Disponible en: http://www.cnbc.com/2015/01/27/cyberterrorists-to-target-critical-infrastructure.html (enlace comprobado el 01-09-2015)

[26] González, M. en EL PAIS. 2014. Disponible en: www.elpais.com/m/politica/2015/02/05/actualidad/1423136881_175042.html (enlace comprobado el 01-09-2015)

[27] Un ataque tipo **DEFACEMENT**, consiste en la modificación de la apariencia de una página web por parte del atacante, bien sea mediante la explotación de un bug de programación o por una mala administración del servidor.

Figura 18. Ejemplo de defacement

Otro ciberataque, ejecutado en este caso por el ISIS en abril de 2015, consistió en una denegación de servicio, DDoS[28], a once canales de la televisión francesa TV5 Monde y el defacement de las cuentas que dicha compañía tenía en las redes sociales. A raíz de estos incidentes, E. Kaspersky declaró que una de las grandes ciberamenazas con las que se enfrenta la sociedad hoy es el ciberterrorismo. Así, continua, mientras los terroristas históricamente no han invertido en ciberataques por que la relación coste beneficio resultaba incierta, recientes informes de inteligencia sugieren que los terroristas han visto el éxito que los criminales han obtenido con sus ciberataques como un indicador de que el tiempo para invertir en los mismos ha llegado[29].

Sea como fuere, los terroristas yihadistas han demostrado que ya tienen ciertas capacidades para poder realizar ciberataques por si mismos, aunque quizás éstas no alcancen para el ataque a una infraestructura crítica no tengan ni las capacidades técnicas ni los conocimientos adecuados para atacar a una infraestructura crítica, sí están mejorando sus capacidades en este

[28] Por un ataque **DDOS** (Denegación de Servicio Distribuida), del inglés (Distributed Denial of Service), se entiende al ataque informático que provoca que un servicio que se presta a través de Internet sea inaccesible a los usuarios legítimos. La forma más frecuente de realizar un DDoS es a través de una botnet. Una botnet es un conjunto de ordenadores y servidores infectados y que son controlados de manera remota.

[29] Steinberg, J. en Forbes. 2015. Disponible en: htpp://onforb.es/1yliZtl (enlace comprobado el 01-09-2015)

campo, pudiendo, además, contratar esos servicios, bien el propio ISIS o bien células locales autónomas, en los dark markets, pudiendo crear un estado de inseguridad muy importante en la sociedad occidental que afectaría, sin lugar a dudas, a la economía.

6.- MONEDAS VIRTUALES O CRITOMONEDAS

6.1.- DEFINICIÓN

Se podrían decir que las monedas virtuales o criptomonedas son un sistema de pago a través de Internet, basadas en un sistema peer-to-peer (P2P o red entre iguales), que contienen un elemento de seguridad basado en la criptografía y en donde el valor es transmitido electrónicamente entre las partes, sin un intermediario.

Las monedas virtuales, por tanto, operan como una moneda en un medio determinado, como es Internet, pero, en realidad, no tienen todos los atributos exigibles a una moneda real, no teniendo sustento legal en la gran mayoría de las legislaciones nacionales. No tienen forma física en billetes o monedas, tan sólo son una cadena de caracteres digitales.

El FinCEN, Agencia del Departamento del Tesoro de los Estados Unidos con la misión de salvaguardar el sistema financiero de la utilización ilícita y blanqueo de dinero, se centra en dos tipos de moneda virtual: la centralizada y la descentralizada.

Centralizada es aquella que son operadas y supervisadas desde un solo punto. Un ejemplo de moneda virtual centralizada sería la Liberty Reserve, que saltó a los medios de comunicación al detener las autoridades estadounidenses a su fundador en el año 2013, definiendo éstos a Liberty Reserve como “el banco de referencia del mundo criminal”, habiendo facilitado el blanqueo de 6000 millones de dólares a través de su sistema de moneda virtual.

En cuanto a moneda virtual descentralizada sería aquella que no tiene un solo punto desde el que es operada o supervisada, siendo el valor enviado o transmitido entre particulares, sin un intermediario.

Entre las características de este tipo de monedas se pueden destacar:

1. Anonimato. El sistema no requiere que las partes prueben su identidad y tenga que ser verificada y validada, como exige la Ley 10/2010 de prevención del blanqueo y financiación del terrorismo, no aportando dato alguno de la identidad de los participantes en la transacción económica. Es evidente que estos niveles de anonimato favorecen a los objetivos de

terroristas, de quienes quieren lavar dinero o llevan a cabo otro tipo de actividades ilegales.

2. Alcance global y sin límite.
3. Velocidad del proceso.
4. No existe la posibilidad de rechazo.
5. Bajo coste. No tiene prácticamente ningún coste o pago de comisiones.
6. Facilidad de uso.
7. Dificultad por parte de las autoridades de seguir o hacer un trazado de las operaciones.
8. Posibilidad de incrementar la seguridad y condiciones de anonimato respecto a un eventual seguimiento por parte de las autoridades mediante el uso de anonimizadores, como puede ser TOR.
9. Falta de regulación. En la actualidad muchos países no han legislado sobre la materia, encontrándose lasa monedas virtuales en una especie de limbo legal.
10. Concurrencia de jurisdicciones. Como ya se trató al hablar de la deep web, la complejidad que permite el uso de redes como TOR para el trabajo de las autoridades en su persecución del delito, los múltiples "saltos" que realizarían las transacciones económicas de las monedas virtuales empleando dicha red harían prácticamente imposible su persecución al entrar en juego múltiples legislaciones nacionales con sus respectivas jurisdicciones.

Como podemos inferir, por las características de las monedas virtuales, éstas tienen un gran potencial y atractivo para que sean empleadas por parte de organizaciones terroristas o de grupos criminales. Tanto es así, que Jennifer Shasky Calvery, Directora de FinCEN, declaró en un foro sobre "Política sobre monedas virtuales" que "lo que la quita el sueño es cuando piensa acerca de las monedas virtuales…la verdadera amenaza que hay ahí fuera, estos días nosotros estamos pensando mucho acerca de ISIL". "Como están ellos moviendo su dinero, y como individuos radicados en los Estados Unidos se convierten en luchadores en el

extranjero: ¿están moviendo su dinero y podemos identificarlos desde los movimientos de su dinero? ¿Qué ocurre si ellos comienzan a mover su dinero a través de bitcoins? Nosotros hemos comenzado a ver algunos artículos publicados que sugieren que esto ya ha ocurrido[30].”

Respecto al número que existe en la actualidad habría que afirmar que es cambiante. Con relativa frecuencia aparecen y desaparecen monedas virtuales, no pudiendo, pues, fijar un número exacto. Como referencia, con bastante fiabilidad, se puede consultar sitios web como puede ser www.coinmarketcap.com, habiendo 606 monedas virtuales en el mes de agosto de 2015, siendo, por volumen, la primera el Bitcoin, seguida de Ripple, y LittleCoin.

Con respecto al tipo de cambio del bitcoins con respecto al resto de las divisas, hay que destacar las grandes fluctuaciones que ha experimentado en su corta historia. Hay quien afirma que es debido a un proceso habitual de oferta y demanda. Por el contrario, hay quien sostiene que hay grandes movimientos especulativos que podrían estar haciendo que la cotización varíe según sus intereses. Lo cierto es que ha variado mucho, pasando de los aproximadamente 10 dólares USA con los que se mantuvo en 2012, a los más de 1100 $ que consiguió en enero de 2014. En la actualidad, en agosto de 2015 se cotiza en torno a los 265 $[31].

6.2.- EL BITCOIN

El Bitcoin es una red consensuada que permite un nuevo sistema de pago y una moneda completamente digital[32]. Esta moneda electrónica, junto a un software y un protocolo, permite la realización de transacciones casi instantáneas entre iguales, ya que se basa en el sistema peer-to-peer (P2P), consiguiendo pagos a nivel mundial con unos costes nulos o muy pequeños al realizar dichas transacciones.

Al operar bajo la tecnología peer-to-peer evita depender de una autoridad monetaria central que sea la responsable de la emisión y el control del dinero, siendo, por tanto, un sistema completamente privado. De esta forma no es posible manipular el valor de los bitcoins o crear

[30] Paganini, P. “The ISIS advances in the DeepWeb among Bitcoin and darknets”. Security Affairs. 2015. Disponible en: http://securityaffairs.co/wordpress/36961/intelligence/isis-in-the-deepweb.html (enlace comprobado el 01-09-2015)

[31] Se puede consultar la cotización en múltiples sitios web como pueden ser en https://blockchain.info/es o en www.coinmarketcap.com

[32] Para saber más acerca del tema se puede consultar: www.bitcoin.org

inflación produciendo más moneda, ya que es la propia red la que gestiona las transacciones y la emisión de los bitcoins, que son generados a través de la llamada minería, de forma controlada y descentralizada[33].

Emplea la criptografía para asegurar y garantizar las transacciones de forma que cada Bitcoin y cada usuario está encriptado con un único identificador, y cada transacción queda registrada y grabada en una especie de libro de contabilidad, conocido como blockchain, que puede ser visto por cualquier usuario de la red, pero que no revela ningún dato personal acerca de las partes que realizaron la transacción económica.

6.2.1.- ORIGEN

Se considera al creador del Bitcoin a un individuo llamado Satoshi Nakamoto que publicó en 2008 un artículo en el que anunciaba que había desarrollado un nuevo sistema de pago electrónico, estando disponible el texto en la dirección web www.bitcoin.org/bitcoin.pdf[34] , basado en el trabajo que, sobre la base de la criptografía de clave pública que daba una solución al problema de los pagos electrónicos había publicado Wei Dai describiendo lo que denominó el b-Money[35].

En 2009 se publico en el portal P2P, nuevamente bajo el nombre de Satoshi Nakamoto, un mensaje del mismo en el que presentaba el portal oficial de Bitcoin, las características fundamentales de esta nueva moneda digital[36].

Respecto al creador del Bitcoin, Satoshi Nakamoto, se encuentra inmerso en un mar de especulaciones, considerándose por mucha gente que no es un individuo, sino un grupo de personas que bajo ese seudónimo han desarrollado esta nueva moneda, llegándose al extremo de quienes consideran que detrás de todo podría estar, en realidad, alguna agencia gubernamental muy poderosa que habría dejado un "puerta trasera" con la que podría

[33] A este respecto se puede consultar el estudio titulado "Bitcoin. Una moneda criptográfica" realizado por el Instituto Nacional de Ciberseguridad (INCIBE). 2014. https://www.incibe.es/CERT/guias_estudios/Estudios//bitcoin_moneda_criptografica

[34] Nakamoto, S. "Bitcoin: A Peer-to-Peer Electronic Cash System". 2008. Disponible en: https://bitcoin.org/bitcoin.pdf (enlace comprobado el 01-09-2015)

[35] Dai, W. "b-Money" Disponible en: www.weidai.com/bmoney.txt (enlace comprobado el 01-09-2015)

[36] Nakamoto, S. "Bitcoin open source implementation of P2P currency". 2009. Disponible en:

htpp://p2pfoundation.ning.com/forum/topics/bitcoin-open-source (enlace comprobado el 01-09-2015)

controlar todo el sistema[37], pero todo lo que hay, hasta el día de hoy, se puede considerar pura especulación.

6.2.2.- COMO FUNCIONA EL BITCOIN

Para empezar a operar con bitcoins lo primero que un usuario tiene que hacer es descargarse lo que se conoce como un monedero virtual, o "wallet", entre las múltiples opciones que se pueden encontrar a día de hoy, pudiendo hacerlo tanto en su ordenador como en dispositivo móvil.

Una vez descargado el monedero virtual se generará una dirección Bitcoin, pudiendo generarse tantas como se deseen, constando dicha dirección de dos partes correlacionadas: una dirección pública, que es con la que el usuario se identifica con el resto; clave privada, que es la que permite autentificarse, accediendo a los fondos que haya en la cartera digital y pudiendo hacer actos de disposición.

Si se quiere enviar bitcoins a otro usuario, tan sólo sería necesario conocer su dirección de Bitcoin pública y con la clave privada del que quiere transferir los bitcoins se firmaría la transacción.

Todo este proceso queda anotado en una contabilidad pública compartida en la que se basa todo el sistema, conocida como cadena de bloques o "block chain". Cualquier transacción confirmada se incluye en la cadena de bloques pudiendo, de este modo, los wallets calcular su saldo disponible y que las transacciones puedan ser verificadas, asegurándose la integridad del sistema e inscribiéndose las transacciones por orden cronológico. Las transacciones deberán ser difundidas entre todos los usuarios y deberán ser confirmadas en la red en los diez minutos siguientes por un proceso conocido como minería.

En este punto hay que introducir otro concepto novedoso como es la minería. Ésta es un sistema de consenso distribuido que se emplea para confirmar transacciones pendientes a ser incluidas en la cadena de bloques. La minería hace cumplir un orden cronológico en la cadena de bloques, protege la neutralidad de la red y permite un consenso entre todos los equipos sobre el estado del sistema. Para confirmar las transacciones estas serán agregadas a un

[37] A este respecto son muy abundantes los artículos periodísticos que se pueden encontrar. Un ejemplo sería: Mathew, J. "Bitcoin 'Conspiracy Theory' Alleges Virtual Currency is NSA or CIA Project" International Business Times" 2014. Disponible en: http://www.ibtimes.co.uk/bitcoin-suspected-be-nsa-cia-project-1460439 (enlace comprobado el 01-09-2015)

bloque que se deberá ajustar a las normas de cifrado y que será verificada por la red. De esta forma se impide que un bloque anterior se modifique, ya que de hacerse quedarían invalidados todos los bloques posteriores, impidiendo, de esta forma, que nadie pueda reemplazar partes de la cadena de bloques para revertir una operación en su propio beneficio.

Con respecto al minero se podría decir que es la persona que pone a disposición la capacidad de procesamiento de su equipo informático para verificar las cadenas de bloques. Pero esto conlleva un coste, por lo que, para hacerlo atractivo, el sistema gratifica al minero que gestiona la producción de un bloque por partida doble: por un lado el sistema le dará una gratificación, que en la actualidad es de 50 bitcoins; y, por otro si hubiese cualquier comisión en las transacciones que se incluyan en el bloque, las mismas podrán ser reclamadas por el productor (minero) de ese bloque. Este sistema es vital para garantizar la integridad del sistema.

En cuanto a cómo conseguir bitcoins, eliminando la posibilidad de obtenerlos por medio de la actividad de la minería, habrá tres formas:

1. Acudir a una casa de cambio virtual o exchanger.
2. Directamente entre particulares. En foros especializados o, incluso, en redes sociales se puede encontrar gente dispuesta a vender o comprar bitcoins, haciendo la transacción cara a cara.
3. Mediante el uso de cajeros automáticos. Se pueden encontrar mapas de ubicación en sitios web como, por ejemplo, www.bitchain.eu o www.coinatmradar.com .

6.2.3.- ANONIMATO

Como se ha explicado anteriormente, la integridad del sistema se basa en que todas las transacciones quedan anotadas en esa suerte de contabilidad pública llamada cadena de bloques por un minero y difundida por toda red, pudiendo ser dicho extremo observado por cualquier usuario de la red en sitios web como https://blockchain.info .

Vamos a ver un ejemplo práctico real haciendo un seguimiento al monedero electrónico que figura en la imagen número 10 en la que un grupo yihadista solicita donativos en bitcoins.

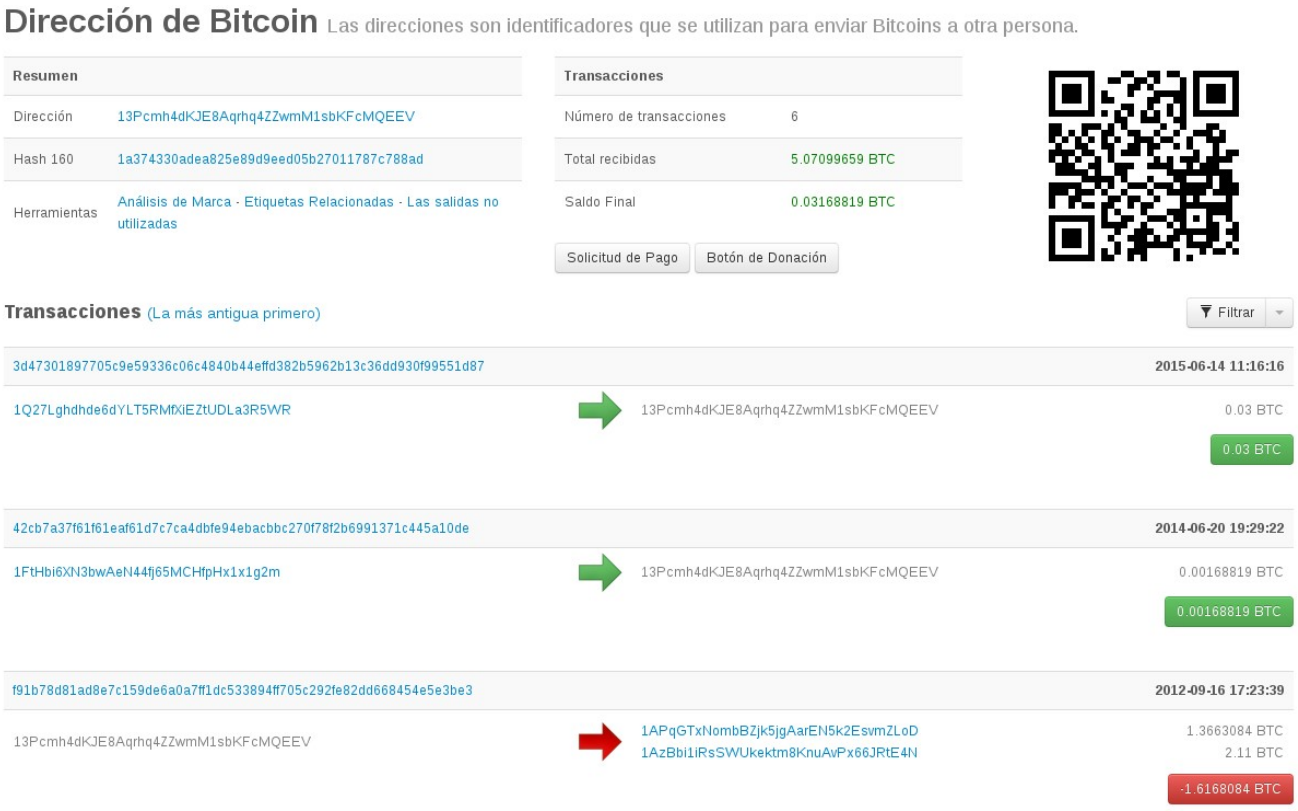

Figura 19. Fuente: www.blockchain.com

En la figura número 19 se puede comprobar que en la dirección que el grupo yihadista propone para realizar donativos en bitcoins figuran una serie de ingresos (los indicados con la flecha verde) y de pagos (con la flecha roja), pudiendo conocer su saldo. Si seguimos el rastro de la dirección a la que han hecho una transferencia de 2.11 BTC:

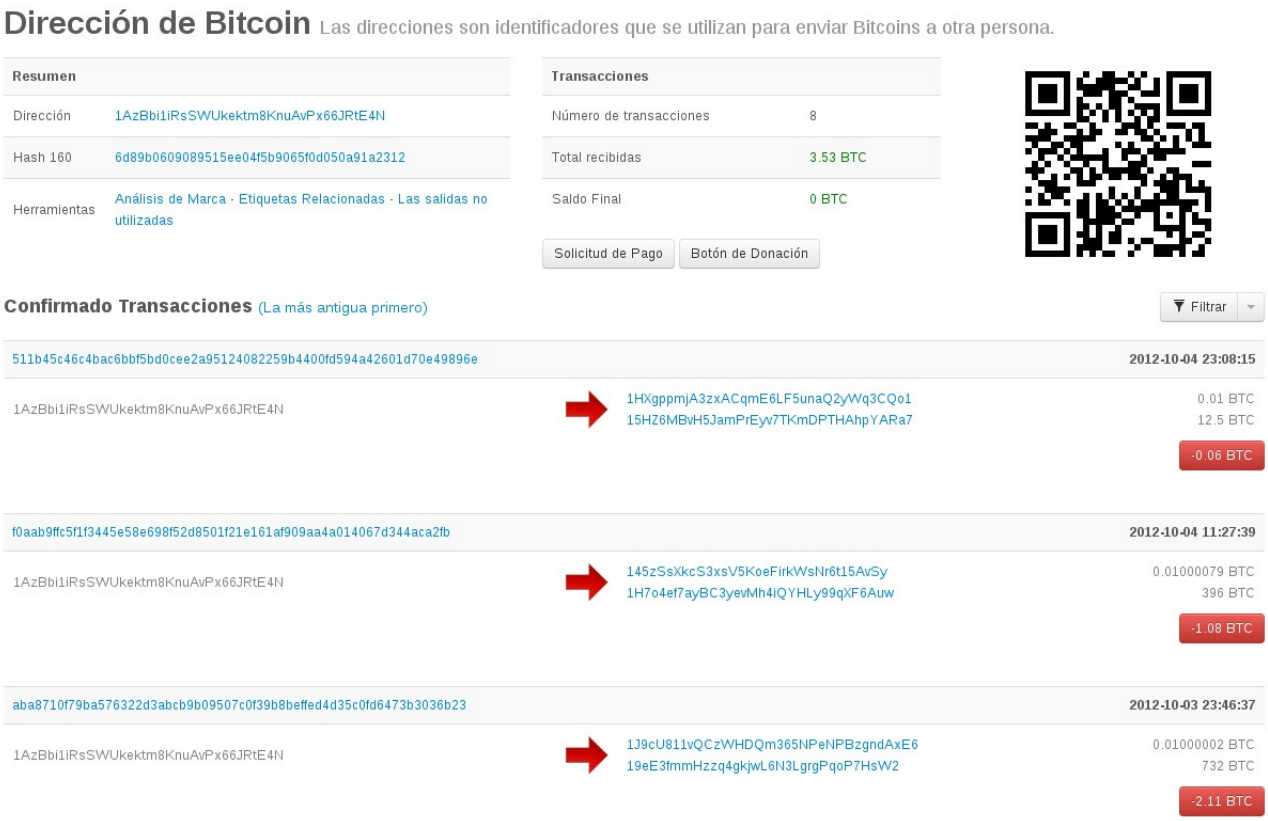

Figura 20. Fuente: www.blockchain.com

Se puede comprobar las transacciones realizadas desde esa dirección, llamando la atención la última transferencia por la cantidad de 732 BTC (más de 190.000 euros al cambio medio de agosto de 2015). Repitiendo la comprobación con esta última dirección:

Figura 21. Fuente: www.blockchain.com

Por último, comprobamos la nueva dirección a la que se la ha hecho la transferencia:

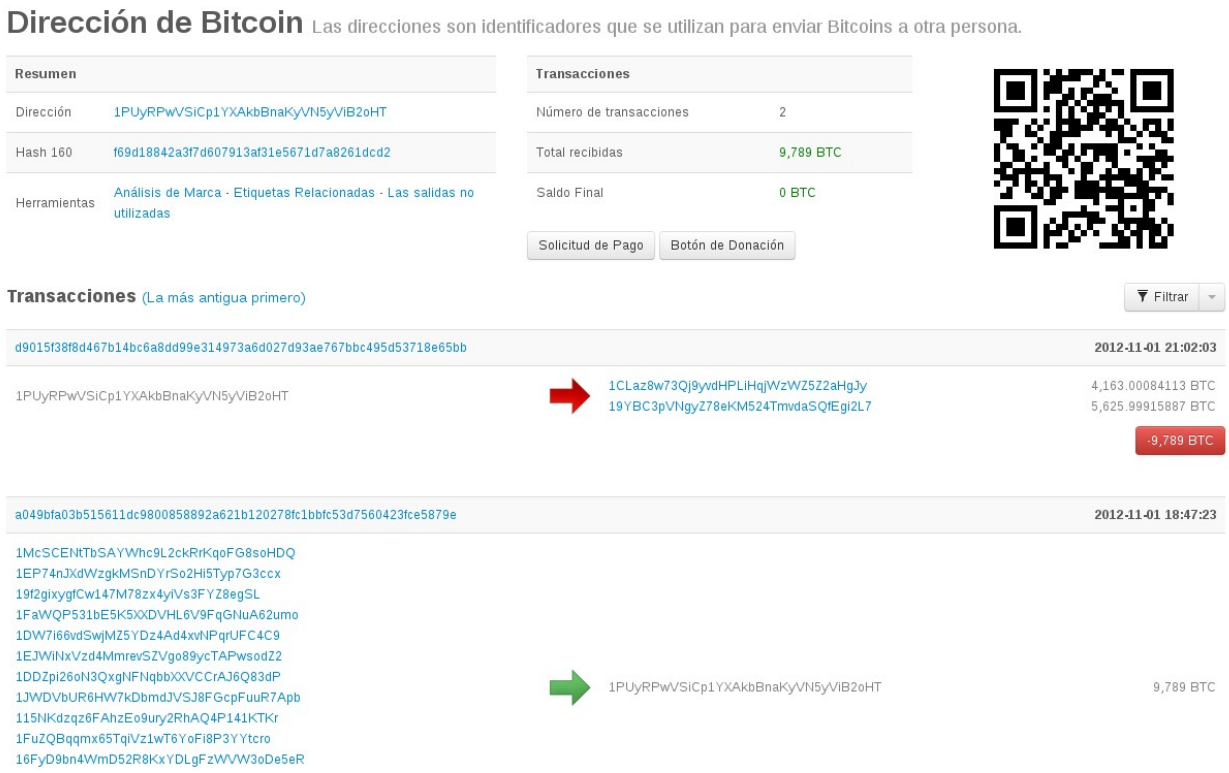

Figura 22. Fuente: www.blockchain.com

Se puede observar que en esta última dirección hay multitud de pagos de pequeña cuantía, pudiendo inferirse que es también es empleada para recibir donativos, destacando que el saldo final asciende a 9789 BTC, o lo que es lo mismo, más de 2.5 millones de euros opacos y dispuestos para ser transferidos a cualquier parte del mundo sin control alguno. Todo ello debería ser objeto, obviamente, de una labor ingente por parte de los servicios o unidades de inteligencia, tratando de desentrañar semejante madeja y conseguir, al fin, identificar a quien se esconde tras esas direcciones.

Antes de avanzar en este apartado habría que distinguir qué sería una transacción anónima y qué sería una transacción privada. Anónima sería aquella operación en la que nadie conoce los datos de identidad de la parte. Privada sería cuando conociendo la identidad de quien realiza una transacción, no se puede determinar ni en cuanto dinero consistió ni por qué bien o concepto se realizó. Así, el dinero en efectivo podría considerarse como un medio privado y anónimo (con las matizaciones que a nivel operativo se pueden plantear, ya que un terrorista

al comprar un bien empleando efectivo podría ser identificado por fotografías por los dependientes, etc.).

Si buscamos una transacción que no es ni anónima ni privada tendríamos que fijar nuestra atención en las compras realizadas con tarjeta de crédito o débito, ya que tanto datos de identificación, como de identificación del comercio quedan registrados.

Las transacciones realizadas en Bitcoin son anónimas, pero no privadas, ya que aunque las identidades no se registran en ninguna parte, todas las transacciones de cada cuenta de Bitcoin queda reflejada en el libro de contabilidad, o block chain, y, como hemos dicho anteriormente, es público, cualquier persona puede acceder al mismo. Además hay quien pone en duda las condiciones de anonimato del Bitcoin, ya que se podría realizar un trazado por conexiones, determinándose desde qué IP´s se han realizado y que podrían facilitar a una agencia o cuerpo policial con el autor de las mismas.

Comenzando por esta última afirmación, si bien son ciertas las dudas de anonimato que se plantean, no es menos cierto que cualquier persona con unos mínimos conocimientos en informática, y más aún elementos pertenecientes a organizaciones terroristas que guardan extremas medidas de seguridad, tiene herramientas fácilmente accesibles para hacer, prácticamente imposible, el rastreo de la conexión. Así, si se realiza la misma empleando en la comunicación la red Tor, y se le añaden más capas que refuercen el anonimato, como puede ser comunicar a través de Tor por medio de una VPN[38], y, además, el empleo de un WIFI público o, mejor aún, una conexión WIFI comprometida[39], la determinación del origen de la comunicación y su autor deviene en, prácticamente, imposible.

Con respecto al posible seguimiento, a través del block chain, de las transacciones realizadas por una determinada cartera de bitcoins, hay servicios o aplicaciones que camuflan o blanquean el origen de los bitcoins, haciendo uso, en la mayoría de los casos, de técnicas muy

[38] VPN es el acrónimo de Virtual Private Network (red privada virtual). Es una red privada construida dentro de una infraestructura de red pública como es Internet. Permite que el ordenador en la red envíe y reciba datos sobre redes públicas como si de una red privada se tratase. Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambas.

[39] WIFI comprometida se trata de conseguir acceso a Internet, de forma inalámbrica por medio de WIFI, pero empleando la red de una persona cuyo router ha sido crakeado, esto es, se han saltado las medidas de seguridad del router pudiendo acceder al mismo libremente. En la actualidad hay multitud de programas y aplicaciones que permiten el crackeo de los routers. Esta práctica no dificulta la determinación de la IP de conexión al investigar un cuerpo policial la misma, pero sí les puede llevar a error, ya que el titular de la conexión no sería quien estaría cometiendo el ilícito penal ni sería la persona objeto de investigación.

similares a las empleadas por los mixers en los dark markets ya descritas anteriormente. Como ejemplo de sitios que dan este servicio podemos encontrar www.bitcoinfog.com o un nuevo protocolo como es zerocash (www.zerocash-project.org).

6.2.4.- USO DEL BITCOIN POR LOS TERRORISTAS

Como hemos citado anteriormente, la directora del FINCen ya declaró que había artículos que sugerían que los terroristas estaban moviendo dinero empleando para ello el Bitcoin. Las agencias de inteligencia creen que elementos terroristas, incluido el ISIS, emplean las diversas oportunidades de transferir dinero a sus operativos en occidente por medio de esta cripto moneda[40].

En este sentido se puede encontrar en la red un blog en pdf titulado "Bitcoin wa Sadaqat al-Jihad" (Bitcoin y la limosna de la lucha física violenta, disponible en https://alkhilafaharidat.files.wordpress.com/2014/07/btcedit-21.pdf ;enlace comprobado el 09-09-2015), que propone que la limosna que los buenos musulmanes deben dar a favor de la lucha se hagan en bitcoins para evitar los controles que los estados kafir imponen en el sistema financiero ordinario, sugiriendo el empleo de la dark wallet para conseguir un total anonimato.

Es indudable que, a día de hoy, los terroristas han fijado su atención en las posibilidades que el Bitcoin les proporciona, haciendo uso del mismo. El citado blog hace referencia explícita al que fue el mayor *black market*, Silk Road, y la posibilidad de comprar armas en el mismo y pagarlas en esta moneda virtual así como la posibilidad de transferir grandes cantidades desde cualquier lugar del mundo a los bolsillos de los mujahideen.

Posiblemente en este punto habría que hacer dos distinciones: la utilidad de esta moneda para organizaciones terroristas como el ISIS; y el empleo de la misma por parte de células locales.

Con respecto al empleo del Bitcoin por parte de una organización terrorista como el ISIS, que controla un vasto territorio y procura la creación de una estructura de estado, el uso de esta moneda no es el más indicado a ese nivel. El ISIS controla pozos de petróleo que vende en los circuitos de mercado negro tradicionales y le proporcionan, según algunas estimaciones, unos

[40] Paganini, P. Obra citada

dos millones de dólares al día[41], a lo que habría que sumar el dinero que obtiene producto del pago de rescates por los secuestros de occidentales y de la venta de las antigüedades que expolian del patrimonio histórico de los lugares que han pasado a controlar[42]. Por tanto, se puede inferir que el ISIS no necesita donaciones y posee suficientes dólares en efectivo para comprar armas pesadas o sufragar operaciones[43] que, difícilmente, se podrían adquirir empleando la moneda virtual a los niveles que dicha organización terrorista, a nivel central, requiere.

En cuanto al uso del Bitcoin por parte de células locales, sí se puede considerar como más que probable su empleo ya que las condiciones de anonimato, inmediatez, ausencia de fronteras y controles legales, facilitan el envío de dinero a operativos que estén radicados clandestinamente en países occidentales o, en sentido contrario, enviar dinero captado en Occidente a las zonas de conflicto, haciendo, casi imposible, a las autoridades locales su localización y monitorización. Estos individuos sí harían uso de ese dinero virtual para obtener productos, como armas y explosivos, en los *black markets*, o para contratar servicios de hacking, pudiendo éstos ser transferidos por el propio ISIS[44] u otra matriz de organización terrorista, bien como producto de donativos recibidos de todas las partes del mundo, o bien obtenidos directamente por ellos mediante el uso fraudulento de numeraciones de tarjetas de crédito, además de otras posibilidades que les facilitan los *black markets*, haciendo de estos sitios en Internet y del Bitcoin elementos básicos para la financiación de las células terroristas. También, como hemos visto anteriormente, esas células locales pueden adquirir productos cotidianos en los, cada vez más abundantes, comercios que aceptan como pago esa moneda o la conversión, por medios que preservan el anonimato, de sus bitcoins en moneda local.

---

[41] Fantz, A. "Venta de petróleo, impuestos, saqueos, extorsiones... así gana dinero ISIS". CNN. 2015. Disponible en: http://cnnespanol.cnn.com/2015/02/20/venta-de-petroleo-impuestos-saqueos-extorsiones-asi-gana-dinero-isis/#0 (enlace comprobado el 01-09-2015)

[42] González, R. "Acuerdo contra el tráfico de antigüedades del ISIS". El País. 2015. Disponible en: http://cultura.elpais.com/cultura/2015/05/18/actualidad/1431936369_795845.html (enlace comprobado el 01-09-2015)

[43] En este sentido: Muadh, Z. "ISIS supporter: the Islamic State does not use Bitcoin. Deepdotweb. 2014. Disponible en: www.deeptoweb.com/2014/09/22/bitcoin-is-not-being-used-by-the-islamic-state/ (enlace comprobado el 01-09-2015)

[44] Klimasinska, K. "Terrorist eyeing Bitcoin, Social Media to Fund Jihad, U.S. says". Bloomberg. 2015. Disponible en: http://www.bloomberg.com/news/articles/2015-06-12/terrorists-eyeing-bitcoin-social-media-to-fund-jihad-u-s-says (enlace comprobado el 01-09-2015)

En esta línea es cada vez más frecuente la aparición de consejos o tutoriales en los que se aconseja el empleo de esta moneda a miembros del ISIS para poder operar de forma anónima, apareciendo noticias, como la del pasado mes de junio de 2015, en la que se informa de la detención de un joven de 18 años en EEUU por estos motivos[45].

Se puede inferir, por tanto, que en la actualidad, y por lo que se conoce en fuentes abiertas, el empleo más usual del Bitcoin está relacionado con la financiación, pero no obsta para que ya se le esté dando otros usos, como los descritos más arriba, y que, posiblemente, tarde aún un tiempo en salir a la luz el verdadero alcance en su uso por organizaciones terroristas.

7.- CONCLUSIONES

En este trabajo se ha analizado la Deep web y las herramientas que pueden resultar útiles a organizaciones terroristas para alcanzar sus objetivos siendo éstas, en muchas ocasiones, idénticas a las de las organizaciones criminales como:

- Mercado negro de bienes digital: conseguir armas, explosivos, documentos falsos, etc, en cualquier lugar del mundo de forma más segura, rápida y con mucha más oferta que el mercado negro tradicional.
- Mercado negro de servicios: contratación de servicios tales como haking, blanqueo de dinero y otros especialistas que fuera de la deep web sólo pocos podrían conseguir mediante contacto directo.
- Servicios financieros: recaudación, gestión y distribución de fondos económicos de forma mucho más segura y con menor riesgo a ser incautada por FFCCS.

En cambio, hay otras necesidades que son cubiertas por la deep web y que resultan exclusivas para organizaciones terroristas como:

- Divulgación de contenidos para propaganda de sus campañas de terror, hacer persistentes esos contenidos que de otro modo las FFCCS podrían bloquear.
- Captación de nuevos miembros.

[45] Oconnell, J. "Virginia teen accused of showing ISIS members how to use Bitcoin". 2015. Disponible en: https://www.cryptocoinsnews.com/virginia-teen-accused-showing-isis-members-use-bitcoin/ (enlace comprobado el 12-09-2015)

- Entrenamiento, instrucción de los nuevos miembros, manuales etc. para lobos solitarios y células aisladas.
- Nuevas formas de ataque directo a infraestructuras críticas, servicios digitales, medios de comunicación etc. Estos ataques tiene al menos el mismo potencial que ataques físicos directos y sin embargo ser mucho más seguros de realizar que éstos para los terroristas

Sin lugar a dudas, las condiciones de anonimato que proporciona la Deep web la configura como un entorno privilegiado para cualquier persona u organización que quiera ocultar su identidad digital al emplear Internet.

Las organizaciones terroristas, en particular las de raíz yihadista, han visto en el uso de la dark web una forma muy segura para poder trabajar en la red pudiendo acceder a comunicaciones encriptadas entre miembros de la organización distribuidos a lo largo del mundo con muy bajo coste; o el acceso a los *black markets* como fuente de financiación de sus células locales y adquisición de armas o explosivos con los que desarrollar sus actividades terroristas; o la captación de fondos a través de los foros provenientes de donaciones[46]. En este punto el desarrollo y expansión de las monedas virtuales y, muy especialmente, el Bitcoin, han añadido un plus en el atractivo que tienen dichos lugares para criminales y terroristas dado el entorno de anonimato y de absoluta seguridad con respecto a eventuales intervenciones de fuerzas policiales.

A día de hoy, la mayor amenaza que se cierne sobre nuestra sociedad proveniente de Internet es, sin duda, el ataque a infraestructuras críticas. El incremento que ha experimentado este tipo de incidentes, a nivel mundial, ha sido exponencial, y, en concreto, en España, según se citó anteriormente, en declaraciones del Ministro de Asuntos Exteriores[47], se ha pasado a ocupar el tercer puesto a nivel mundial en 2014 por este tipo de incidentes.

Es posible que las organizaciones terroristas aún no hayan alcanzado un nivel técnico lo suficientemente alto como para planificar y ejecutar este tipo de atentados empleando Internet, pero lo cierto es que los terroristas van avanzando en sus capacidades técnicas en este campo pudiendo, además, recurrir al conocido como "*crime as a service*", y contratar a

[46] EUROPOL. TE-SAT 2015 (European Union Terrorism Situation and Trend Report). Página 9. Disponible en https://www.europol.europa.eu/content/european-union-terrorism-situation-and-trend-report-2015 (enlace comprobado el 01-09-2015)

[47] Ver cita número 26

quien sí tiene esas capacidades y que las oferta dentro de la dark web y que cobraría sus servicios en Bitcoins.

Por todo ello, la investigación del uso que dan las organizaciones terroristas de la dark web constituye una prioridad para agencias de inteligencia y fuerzas policiales, contando con múltiples dificultades, dada su propia naturaleza, con el empleo de canales de comunicación encriptados que hacen prácticamente imposible su monitorización.

Respecto a las monedas virtuales existe a día de hoy un auténtico desconcierto con respecto a su tratamiento. Mientras que hay países como Estados Unidos que están tratando de regularla, otros países han optado por prohibirlas[48], pero lo cierto es que su uso escapa al control de las autoridades y en países en los que se ha optado por su prohibición, como China o la India, el uso del Bitcoin sigue siendo el mismo.

Las monedas virtuales sirven para la financiación del terrorismo, como hemos podido ver, anteriormente, en un supuesto real, en el que obtenían más de 2.5 millones de euros con pequeños donativos que escapan, absolutamente, del control de cualquier agencia policial o de inteligencia.

Además facilita el lavado de dinero, ocultando el origen de los fondos por medio de herramientas como la conocida como dark wallet, que mezcla los bitcoins provenientes de distintas transacciones sin que sea, finalmente, posible determinar el origen de los mismos.

También sirve esta moneda para la adquisición de armas, explosivos o cualquier otro elemento que sirva para la planificación, preparación y ejecución de una acción terrorista en los *black markets*, haciendo muy difícil, por los motivos que se han detallado en este trabajo, la detección y actuación por parte de las autoridades policiales. Además, la expansión que está experimentando el Bitcoin en algunos países, como puede ser España, hace que se admita en comercios y restaurantes, lo que facilitaría que una célula local pudiese establecerse en una ciudad concreta y realizar los pagos diarios con dicha criptomoneda, sin tener que obtener divisa que sí este sometida a control, por lo que los márgenes de seguridad que consiguen ante una eventual detección policial de los mismos se incrementa.

Dado lo reciente de la creación del Bitcoin, 2008, en la actualidad hay muy pocos datos en fuente abierta acerca del empleo real por parte de las organizaciones terroristas de la misma,

[48] Martínez, A. "10 países en los que Bitcoin está prohibido". Diariobitcoin. 2015. Disponible en: http://www.diariobitcoin.com/index.php/2015/05/27/10-paises-en-los-que-bitcoin-esta-prohibido/ (enlace comprobado el 01-09-2015)

no conociéndose incautación alguna a elementos terroristas. Esto no significa que no se esté empleando de forma regular por los mismos, como hemos demostrado en la campaña de los donativos en bitcoins que han supuesto más de 2.5 millones de euros al cambio, más bien al contrario, que su propia naturaleza hace muy complicada la detección e intervención de los mismos. Cabe recordar que la primera incautación de bitcoins la realizó el FBI en el año 2013 en el marco de la operación que propició el cierre del, hasta ese momento, mayor *black market* existente, Silk Road[49], y que el Cuerpo Nacional de Policía realizó poco después la que resultó ser la segunda incautación de esa moneda virtual, en el marco de la operación Ransom, más conocida como el "virus de la Policía"[50]. A partir de ahí las operaciones policiales que dado como fruto la incautación de Bitcoins son muy escasas.

En resumen, la conjunción Deep/dark web y Bitcoin plantea un reto de gran complejidad a las agencias de inteligencia y fuerzas policiales en cuanto a su investigación. Su propia naturaleza hace que las legislaciones nacionales sean insuficientes para dicha tarea, siendo imprescindible acomodarlas a un entorno internacional que emplee similares armas jurídicas para combatirlas, creando un marco jurídico homogéneo, y que la cooperación entre todos los actores involucrados en la persecución sea franca y decidida.

[49] Pareja, P., "El FBI detiene al administrador de Silk Road, el eBay de las drogas". El País. 2013. Disponible en: http://sociedad.elpais.com/sociedad/2013/10/02/actualidad/1380739522_500017.html (enlace comprobado el 12-09-2015)

[50] Diario El Mundo citando información de la Agencia EFE. Disponible en: http://www.elmundo.es/elmundo/2013/02/14/navegante/1360826212.html (enlace comprobado el 12-09-2015)

BIBLIOGRAFÍA

Ashley, Sean P., "The future of Terrorist Financing: Fighting terrorist financing in the digital Age", Penn State Journal of International Affairs. (2012). Páginas 9-26

Bergman, Michael K "The Deep Web: surfacing hidden value" 2001. Disponible en http://grids.ucs.indiana.edu/courses/xinformatics/searchindik/deepwebwhitepaper.pdf (enlace comprobado el 1-09-2015)

Biddle, P., England P., Peinado M. y Willman B., "The Darknet and the Future of Content Distribution". Microsoft Corporation. Disponible en: http://msl1.mit.edu/ESD10/docs/darknet5.pdf (enlace comprobado el 01-09-2015)

Buniller, E. y Shanker, T., Panetta warns of dire threat of cyberattack on U.S.". The New York Times. 2012. Disponible en: http://mobile.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?_r=1&referrer= (enlace comprobado el 01-09-2015)

Curthbertson, A. "HORNET: TOR-style dark web networks allows high-speed anonymus web browsing" International Business Times. 2015. Disponible en: http://www.ibtimes.co.uk/hornet-tor-style-dark-web-network-allows-high-speed-anonymous-web-browsing-1512359 (enlace comprobado el 01-09-2015)

Dai, W. "b-Money" Disponible en: www.weidai.com/bmoney.txt (enlace comprobado el 01-09-2015)

Ellyatt, H. "Cyberterrorits to target critical infrastructure". CNBC. 2015. Disponible en: http://www.cnbc.com/2015/01/27/cyberterrorists-to-target-critical-infrastructure.html (enlace comprobado el 01-09-2015)

Estrategia de Ciberseguridad Nacional. Presidencia del Gobierno de España. 2013. Disponible en: http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf (enlace comprobado el 01-09-2015)

EUROPOL. TE-SAT 2015 (European Union Terrorism Situation and Trend Report). Página 9. Disponible en https://www.europol.europa.eu/content/european-union-terrorism-situation-and-trend-report-2015 (enlace comprobado el 01-09-2015)

Fantz, A. “Venta de petróleo, impuestos, saqueos, extorsiones... así gana dinero ISIS”. CNN. 2015. Disponible en: http://cnnespanol.cnn.com/2015/02/20/venta-de-petroleo-impuestos-saqueos-extorsiones-asi-gana-dinero-isis/#0 (enlace comprobado el 01-09-2015)

Fisher, D. “¿Qué es TOR?”. Blog Kaspersky. 2013. Disponible en: https://blog.kaspersky.es/que-es-tor/716/ (enlace comprobado el 01-09-2015)

Glasser, S. y Coll, S. “The Web as Weapon” The Washington Post. 2005. Disponible en: http://www.washingtonpost.com/wp-dyn/content/article/2005/08/08/AR2005080801018.html (enlace comprobado el 01-09-2015)

González, M. en EL PAIS. 2014. Disponible en: www.elpais.com/m/politica/2015/02/05/actualidad/1423136881_175042.html (enlace comprobado el 01-09-2015)

González, R. “Acuerdo contra el tráfico de antigüedades del ISIS”. El País. 2015. Disponible en: http://cultura.elpais.com/cultura/2015/05/18/actualidad/1431936369_795845.html (enlace comprobado el 01-09-2015)

Instituto Nacional de Ciberseguridad. “Anonimato e Internet. ¿Ilusión o realidad? Navegando en la deep web”. 2013. Disponible en: https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/anonimato_internet_deep_web (enlace comprobado el 01-09-2015)

Instituto Nacional de Tecnología de las Comunicaciones, INTECO. “Bitcoin. Una moneda criptográfica”. Disponible en: https://www.incibe.es/CERT/guias_estudios/Estudios//bitcoin_moneda_criptografica

Jacobson, M., “Terrorist Financing on the Internet”. CTC Sentinel. June 2009. VoL 2. Issue 6. Página 18

Jordán, J. “El terrorismo en la sociedad de la información. El caso de Al Qaida”. El profesional de la información, volumen 11, número 4, julio-agosto 2002. Página 300 (citando a Arquilla, Ronfeldt, Zanini, 1999 “Networks, netwar and information age terrorism”. Rand, Santa Monica.

Klimasinska, K. “Terrorist eyeing Bitcoin, Social Media to Fund Jihad, U.S. says”. Bloomberg. 2015. Disponible en: http://www.bloomberg.com/news/articles/2015-06-12/terrorists-eyeing-bitcoin-social-media-to-fund-jihad-u-s-says (enlace comprobado el 01-09-2015)

Leetaru, K. Citado por Daileda, C. y Franceschi-Bicchierai, L. “U.S. Intelligence Officials want ISIL fighters to keep Tweering”. Marshable. 2014. Disponible en: http://mashable.com/2014/07/11/us-wants-iraq-radicals-to-tweet/ (Enlace comprobado el 01-09-2015)

Martínez, A. “10 países en los que Bitcoin está prohibido”. Diariobitcoin. 2015. Disponible en: http://www.diariobitcoin.com/index.php/2015/05/27/10-paises-en-los-que-bitcoin-esta-prohibido/ (enlace comprobado el 01-09-2015)

Mathew, J. “Bitcoin 'Conspiracy Theory' Alleges Virtual Currency is NSA or CIA Project” International Business Times” 2014. Disponible en: http://www.ibtimes.co.uk/bitcoin-suspected-be-nsa-cia-project-1460439 (enlace comprobado el 01-09-2015)

Muadh, Z. “ISIS supporter: the Islamic State does not use Bitcoin. Deepdotweb. 2014. Disponible en: www.deeptoweb.com/2014/09/22/bitcoin-is-not-being-used-by-the-islamic-state/ (enlace comprobado el 01-09-2015)

Nakamoto, S. “Bitcoin: A Peer-to-Peer Electronic Cash System”. 2008. Disponible en: https://bitcoin.org/bitcoin.pdf (enlace comprobado el 01-09-2015)

Nakamoto, S. “Bitcoin open source implementation of P2P currency”. 2009. Disponible en: htpp://p2pfoundation.ning.com/forum/topics/bitcoin-open-source (enlace comprobado el 01-09-2015)

Oconnell, J. “Virginia teen accused of showing ISIS members how to use Bitcoin”. 2015. Disponible en: https://www.cryptocoinsnews.com/virginia-teen-accused-showing-isis-members-use-bitcoin/ (enlace comprobado el 12-09-2015)

Paganini, P. “The ISIS advances in the DeepWeb among Bitcoin and darknets”. Security Affairs. 2015. Disponible en: http://securityaffairs.co/wordpress/36961/intelligence/isis-in-the-deepweb.html (enlace comprobado el 01-09-2015)

Pareja, P., “El FBI detiene al administrador de Silk Road, el eBay de las drogas”. El País. 2013. Disponible en: http://sociedad.elpais.com/sociedad/2013/10/02/actualidad/1380739522_500017.html (enlace comprobado el 12-09-2015)

Proyecto del Internet Invisible se puede consultar el enlace https://geti2p.net/es/ (enlace comprobado el 01-09-2015)

Proyecto TOR. Se puede consultar el enlace: https://www.torproject.org/ (Enlace comprobado el 01-09-2015). Respecto a los Hidden Services del Proyecto TOR se puede consultar

https://www.torproject.org/docs/tor-hidden-service.html.en (Enlace comprobado el 01-09-2015)

Steinberg, J. en Forbes. 2015. Disponible en: htpp://onforb.es/1yliZtl (enlace comprobado el 01-09-2015)

Torres Soriano, M., "El eco del terror. Ideología y propaganda en el terrorismo yihadista". Madrid: Plaza y Valdés. (2009). Páginas 149 y siguientes.

Torres Soriano, M. "Terrorismo yihadista y nuevos usos de Internet: la distribución de propaganda". Real Instituto Elcano. ARI número 110/2009

UNDOC (Oficina de las Naciones Unidas contra la Droga y el Delito) "El uso de internet con fines terroristas" 2013. Disponible en: http://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/Use_of_Internet_Ebook_SPANISH_for_web.pdf (enlace comprobado el 01-09-2015).

Weimann, G. "Terror on the Internet: The New Arena, The New Challenges" United States Institue of Peace. 2004. Disponible en: http://www.usip.org/events/terror-the-internet-the-new-arena-the-new-challenges (enlace comprobado el 01-09-2015)